Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»
Національна бібліотека України імені В. І. Вернадського

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 11 (листопад)

Київ – 2022

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2022.– №11 (листопад). – 393 с.

Заснований Науково-дослідним інститутом інформатики і права Національної академії правових наук України та Національною бібліотекою України імені В.І. Вернадського у 2017 р. Видається щомісяця. Відповідальний редактор О. Довгань. Упорядники О. Довгань, Л.Литвинова, С.Дорогих. Дизайн обкладинки С.Дорогих.

Аналітичний дайджест покликаний надати інформацію з питань кібербезпеки, що є надзвичайно актуальними в контексті розвитку інформаційного суспільства, зростання кіберзлочинності, використання засобів кібертероризму у гібрідних війнах та необхідності розбудови системи забезпечення кібернетичної безпеки України відповідно до визначених стратегічних напрямків з урахуванням тенденцій розвитку кіберпростору, сучасних викликів та загроз його безпеці. Призначення дайджесту – ознайомлення широкого кола фахівців у сфері кібербезпеки, а також і всіх користувачів, які цікавляться цією проблематикою, з інформаційними джерелами мережі Інтернет та новими надходженнями до фондів НБУВ (монографії, автореферати дисертацій, підручники, збірники наукових праць, матеріали міжнародних конференцій, статті з періодичних видань), що висвітлюють сучасні проблеми кібербезпеки в Україні та за кордоном.

Ознайомитися з літературою із фондів НБУВ та онлайновими інформаційними ресурсами можна за адресою: проспект Голосіївський, 3, м. Київ, 03039.

© Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», 2022
© Національна бібліотека України імені В.І. Вернадського, 2022

ЗМІСТ

Стан кібербезпеки в Україні 4
Правове забезпечення кібербезпеки в Україні 4
Кібервійна проти України 4
Боротьба з кіберзлочинністю в Україні 17
Міжнародне співробітництво у галузі кібербезпеки 23
Світові тенденції в галузі кібербезпеки 28
Сполучені Штати Америки 77
Країни ЄС та Великобританія 124
Австралія та Нова Зеландія 142
Російська Федерація та країни ЄАЕС 146
Інші країни 147
Кібервійни та протидія зовнішній кібернетичній агресії 158
Кіберстрахування 182
Кіберзахист критичної інфраструктури 187
Кіберзахист закладів охорони здоров’я 196
Захист персональних даних та соціальні мережі 206
Кіберзлочинність та кібертерроризм 254
Діяльність хакерів та хакерські угруповування 273
Вірусне та інше шкідливе програмне забезпечення 274
Фішингові атаки 336
Операції правоохоронних органів та судові справи проти кіберзлочинців 339
Технічні аспекти кібербезпеки 361
Виявлені вразливості технічних засобів та програмного забезпечення 362
Технічні та програмні рішення для протидії кібернетичним загрозам 381

Правове забезпечення кібербезпеки в Україні

«Президент України Володимир Зеленський підписав ухвалений Верховною Радою закон, який посилить сферу захисту критичної інфраструктури, повідомляє Держспецзв'язку.

Згідно з документом, Державна служба спеціального зв'язку та захисту інформації України виконуватиме функції уповноваженого органу з питань захисту критичної інфраструктури під час дії воєнного стану, а також протягом 12 місяців після його припинення чи скасування.

У Держспецзв'язку наголосили, що в умовах повномасштабної війни Росії проти України та постійних ворожих атак захист об'єктів критичної інфраструктури (ОКІ) та об'єктів критичної інформаційної інфраструктури (ОКІІ), які на них розміщені, є пріоритетними для держави.

«Вже триває робота над створенням переліку ОКІ. Також буде сформовано та наповнено реєстр об'єктів критичної інформаційної інфраструктури. Це дасть можливість проаналізувати рівень їхньої захищеності та посилити стійкість там, де необхідно, ефективніше виявляти загрози та запобігати їм, забезпечувати постійний і надійний захист таких об'єктів», – розповів голова Держспецзв'язку Юрій Щиголь.

У повідомлені зазначено, що нові повноваження дозволять Держспецзв'язку покращити ефективну взаємодію з іншими суб'єктами національної системи захисту критичної інфраструктури…» ***(В Україні посилять кіберзахист: президент підписав закон // Українські медійні системи (https://glavcom.ua/country/politics/v-ukrajini-posiljat-kiberzakhist-prezident-pidpisav-zakon-886959.html). 04.11.2022).***

***

Кібервійна проти України

«Исследователь России Крис Миллер о переоценке России и недооценке Украины

Крис Миллер, доцент школы Флетчера Университета Тафтса

С момента начала войны против Украины в феврале 2022 года экономика России сократилась, и она предприняла усилия по сокращению экономики Украины и западных союзников. Но «российские вооруженные силы недостаточно эффективны», — говорит доктор Крис Миллер, адъюнкт-профессор международной истории и автор книг по истории России. Он говорит, что и Россия, и Запад переоценили способность страны «эффективно использовать свои возможности».

«Мы недооценили возможности Украины, — говорит Миллер. С точки зрения кибербезопасности, по его словам, «украинская оборона и неисправные российские наступательные системы» являются причиной того, что «не было никаких очень успешных... кибератак против Украины».

В этом выпуске «Cybersecurity Unplugged» Миллер обсуждает:

успешные усилия Украины по улучшению своей кибербезопасности;

проблемы кибербезопасности, стоящие перед США, и то, как образование положительно влияет на оборону;

«критическая и незаменимая роль» США в предоставлении программного обеспечения и инструментов, которые делают возможным развитие технологического сектора.

Миллер — адъюнкт-профессор международной истории в Школе Флетчера Университета Тафтса. Его исследования сосредоточены на российской истории, политике и экономике. Он также является автором книг «Путиномика: власть и деньги в возрождающейся России» и «Мы будем хозяевами: повороты России в Восточную Азию от Петра Великого до Путина». ***(Steve King. The Role of Cybersecurity in the Russia-Ukraine War // Information Security Media Group, Corp. (https://www.govinfosecurity.com/interviews/role-cybersecurity-in-russia-ukraine-war-i-5174). 09.11.2022).***

***

«Хактивисты называют ЦБ РФ и Альфа-банк жертвами

Украинская группа добровольцев-хактивистов утверждает, что украла 27 000 файлов из российского центрального банка.

IT-армия Украины заявила в четверг, что все 2,6 гигабайта файлов доступны на Anonfiles, а в Telegram-аккаунте министра цифровой трансформации Украины Михаила Федорова появилась новость о взломе.

«У нас есть много интересной информации о кадрах, специализированных автоматизированных банковских системах, их выходных файлах, принципах их взаимодействия, системах КПЭ и других материалах, которые циркулируют в сетях ЦБ РФ», — Telegram-канал Федорова состояния.

Данные, к которым получила доступ украинская хакерская группа, включали детали финансовых транзакций Минобороны России и данные военнослужащих, такие как номера телефонов и карт.

Российское государственное информационное агентство ТАСС опубликовало опровержение, в том числе заявление Банка России о том, что никакого взлома не было и что рассматриваемые документы уже были доступны в Интернете.

Армия информационных технологий в понедельник также заявила, что нарушила обработку платежей в Альфа-банке, частном финансовом учреждении, базирующемся в Москве.

В понедельник Forbes Russia сообщил, что инвестиционные клиенты Альфа-Банка в России не могут получить доступ к своим портфелям.

С тех пор, как в феврале началось российское вторжение в Украину, киберпространство превратилось в прокси-зону конфликта, хотя и в меньших масштабах, чем многие изначально опасались. Августовский отчет Института кибермира показал, что с начала войны Украина подверглась 114 случаям кибератак, в то время как Россия пострадала 102 раза». ***(Akshaya Asokan. IT Army of Ukraine Targets Russian Banks // Information Security Media Group, Corp.***

(https://www.govinfosecurity.com/army-ukraine-targets-russian-banks-a-20443). 09.11.2022).

***

«Темпы российских кибератак против Украины значительно возросли после ее незаконного вторжения в феврале 2022 года с целью подорвать суверенитет и стратегическое преимущество Украины в войне.

Министр иностранных дел Великобритании Джеймс Клеверли сообщил, что Великобритания предоставила Украине пакет поддержки в размере 6,35 млн фунтов стерлингов, чтобы помочь защитить ее критически важную национальную инфраструктуру и жизненно важные государственные службы от кибератак.

Британская «Украинская киберпрограмма» была мобилизована вскоре после вторжения Путина в феврале для защиты от участившихся российских кибератак. Программа до сих пор не была обнародована для защиты ее операционной безопасности.

Используя опыт ведущих поставщиков кибербезопасности, программа на сегодняшний день оказывает поддержку в реагировании на инциденты государственным органам Украины, защищая их от разрушительных кибератак, включая вредоносные программы, такие как Industroyer2. Это предотвращает доступ злоумышленников к жизненно важной информации, имеющей отношение к военным усилиям. Программа также ограничила доступ злоумышленников к жизненно важным сетям и помогла Украине защитить свою критически важную инфраструктуру от будущих атак. Кроме того, Великобритания поставила передовые аппаратные и программные средства кибербезопасности, включая брандмауэры для предотвращения атак; Защита от DDoS-атак, чтобы граждане Украины могли продолжать получать доступ к жизненно важной информации; и возможности судебной экспертизы, позволяющие украинским аналитикам полностью понять компрометацию системы.

«Атака России на Украину не ограничивается ее ужасающим вторжением на территорию» — сказал Джеймс Клеверли. «Он также настойчиво пытался вторгнуться в киберпространство Украины, угрожая важной информации, услугам и инфраструктуре».

Министр иностранных дел заявил, что поддержка Украины со стороны Великобритании не ограничивается военной помощью. «Мы используем передовой британский опыт для поддержки киберзащиты Украины. Вместе мы обеспечим поражение Кремля во всех сферах: на земле, в воздухе и в киберпространстве».

Линди Кэмерон, генеральный директор Национального центра кибербезопасности, сказала, что центр гордится тем, что сыграл свою роль в поддержке украинских киберзащитников. «Они установили впечатляющую защиту от российской агрессии в киберпространстве, точно так же, как они сделали это на поле боя. Угроза остается реальной, и пакет поддержки Великобритании, несомненно, еще больше укрепляет обороноспособность Украины».

Российские субъекты имеют долгую историю враждебной и дестабилизирующей деятельности против Украины, в том числе:

Отключение части электросети Украины в декабре 2015 года, в результате чего 230 000 человек остались без электричества на срок до шести часов.

Разрушительные кибератаки в 2017 году, направленные против финансового и энергетического секторов Украины и государственных служб, привели к цепным последствиям для других европейских партнеров.

Работа киевского метрополитена и аэропорта Одессы были нарушены программами-вымогателями, которые шифровали жесткие диски.

DDoS-атаки 15–16 февраля 2022 года, которые, по мнению Национального центра кибербезопасности, были делом рук российской военной разведки ГРУ.

Серия кибератак после вторжения, в том числе против коммерческих операторов, таких как Viasat, в марте, серьезно повлияла на доступ к Интернету и другим услугам как в Украине, так и в других частях Европы.

Темпы российских кибератак против Украины значительно возросли после ее незаконного вторжения в феврале 2022 года с целью подорвать суверенитет и стратегическое преимущество Украины в войне». ***(U.K. Reveals £6 Million Cybersecurity Support Package to Ukraine // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/u-k-reveals-6-million-cybersecurity-support-package-to-ukraine/). 01.11.2022).***

***

«Україна відбиває атаки та переходить у кібернаступ.

Крім ракетних ударів, Росія проводить потужні кібератаки на українські енергооб'єкти, щоб спричинити максимальний блекаут. Україні, втім, вдається їх відбивати і навіть переходити у кіберконтрнаступ.

Про це заявив начальник Департаменту кібербезпеки СБУ Ілля Вітюк в інтерв'ю Liga.net.

«Енергетика, інфраструктура і логістика – це пріоритетні цілі для російських спецслужб. Останні обстріли ТЕЦ супроводжувалися і кібератаками. Ми очікували на такий сценарій, тому жодна з них не була ефективною.

Інколи ми маємо інформацію, куди битиме ворог найближчими днями чи тижнями, і наша задача – не допустити цього. Про більшість кібератак суспільство не знає, але Росія сьогодні робить в середньому понад 10 кібератак на добу».

За словами Вітюка, якби їх не відбивали, то наслідки були б «украй серйозними».

Він пояснив, що кібератаки можуть бути набагато ефективнішими та дешевшими за ракетні обстріли, адже одночасна атака на всі обленерго може спричинити вимкнення світла по всій країні.

Він додав, що наразі у найгірших випадках через кібератаки росіян можуть вимкнути електроенергію на 5-10 хвилин або зупинити на короткий час роботу деяких сервісів. Але Департамент кібербезпеки Служби безпеки працює над тим, щоб навіть такого не ставалося.

За словами Вітюка, приблизно 90% всіх кібератак на українські державні ресурси здійснюють спецслужби РФ. Ще невеликий відсоток кібератак – це справа рук білоруських спецслужб, які сприяють РФ. І до 1% – це злочинні зусилля решти спецслужб.

Він додав, що зазвичай це не деструктивні атаки, а спроби отримати певну розвідінформацію.

Кількість атак за останні роки лише зростає: якщо у 2020 році було зафіксовано близько 800 кібератак, то у 2021-му – майже 1400, а цього року – вже понад 3500.

«Ми вже до всього готові, немає нічого такого, що б ми не бачили», – каже Вітюк.

Україна розпочала кіберконтрнаступ уже 24 лютого.

Раніше Україна не вдавалася до кібернаступу, тому що такі дії, з точки зору міжнародних норм, могли бути розцінені як привід для війни. «Сьогодні наш контрнаступ розвивається ще блискавичніше, ніж на традиційному фронті. Часто палає і кібербавовна», – сказав Вітюк.

Він також додав, що фактично в Україні є своя кібертероборона, яка налічує сотні тисяч бійців – цивільних українців, які долучилися до боротьби на кіберфронті…» ***(СБУ: Росія щодня здійснює з десяток кібератак на енергооб'єкти України // ДМ media sapiens (https://ms.detector.media/kiberbezpeka/post/30629/2022-11-09-sbu-rosiya-shchodnya-zdiysnyuie-z-desyatok-kiberatak-na-energoobiekty-ukrainy/). 09.11.2022.)***

***

«Держспецзв'язку фіксує подальше зростання кількості кіберінцидентів та кібератак на державні інформаційні ресурси та об’єкти критичної інформаційної інфраструктури від початку війни.

Про це йдеться у квартальному звіті відомства.

Зазначається, що у 3 кварталі 2022 року за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було опрацьовано 24 млрд подій інформаційної безпеки (ІБ).

При цьому кількість зареєстрованих та опрацьованих кіберінцидентів зросла - від 64 до 115 порівняно з попереднім кварталом.

Основною метою хакерів є кібершпіонаж, порушення доступності державних інформаційних сервісів та знищення даних інформаційних систем.

Фахівці Державного центру кіберзахисту зафіксували істотне зростання розповсюдження шкідливого програмного забезпечення, яке дає можливість хакерам викрадати дані чи й взагалі знищувати їх, - підкреслюють в Держспецзв'язку.

Порівняно з попереднім кварталом, кількість подій ІБ з високим рівнем критичності зросла у 3,8 рази, кількість зареєстрованих кіберінцидентів із високим рівнем критичності зросла на 128%.

За ці місяці кількість критичних подій ІБ, джерелом яких є IP-адреси Росії, зросла у 35 разів, порівняно з першим та другим кварталами року.

Також, порівняно з другим кварталом, майже вдвічі зросла кількість детектованих подій ІБ, пов’язаних із активним скануванням, джерелом яких є IP-адреси Росії. Саме з цих IP здійснювали кібератаки на українські інформаційні ресурси, розповсюджували фейкову інформацію, спрямовану на дискредитацію державних органів під час російсько-української війни тощо, - йдеться у звіті.

За атрибуцією абсолютна більшість кіберінцидентів пов’язана з хакерськими угрупуваннями, що фінансуються урядом РФ. Зокрема, це UAC-0010 (Gamaredon) та інші.

Підкреслюється, що у 3 кварталі 2022 року основною мішенню хакерів із РФ були фінансовий та комерційний сектори, а також українські державні та місцеві органи влади.

«Найбільшу частку подій інформаційної безпеки можна пов’язати з APT-угрупуваннями та хактивістами», - додали у відомстві». ***(Олексій Павлиш. Кількість кібератак на Україну продовжує зростати – Держспецзв'язку // Економічна правда (https://www.epravda.com.ua/news/2022/11/10/693694/). 10.11.2022).***

***

«Українські кіберфахівці зруйнували міф про «непереможних російських хакерів» та пішли у контрнаступ, зазначає політичний експерт Олексій Голобуцький.

Водночас агентура рф продовжує розкручувати в Європі тему кіберзагроз, хоча насправді росіяни зазнають поразок на кіберфронті.

«Війна в Україні зруйнувала міф про «непереможних російських хакерів», як і «про другу армію в світі» і про інші «аналоговнєти»... Кібербезпека росіян поступово рухається «строго по плану в хаотическом порядке» на інший берег Дніпра», - вважає Олексій Голобуцький.

Він зазначив, що кіберфахівці СБУ з початку лютого відбили вже понад 3,5 тис. кібератак на інформаційні ресурси, реєстри та органи влади.

«Київ, як і інші міста-мільйонники, хотіли залишити без світла і води ще у вересні. Тоді ж – «покласти» онлайн-банкінг та будь-які платежі в інтернеті. Як бачимо, не вийшло – наші кіберфахівці спрацювали краще. Зараз СБУ відбиває в середньому по 10 атак в день і встигає наваляти у відповідь", - наводить статистику експерт.

Водночас, українські кіберфахівці не лише обороняються, але й ідуть у наступ. Експерт наводить приклади, коли українська IT-армія отримала доступ до системи енергетичної компанії у ленінградській області. Тоді ряд міст у рф сиділи при свічках. Також українські хакери зламали базу Центробанку рф, виклавши у відкритий доступ його бази даних». ***(Кіберфахівці СБУ довели, що «непереможні російські хакери» – це міф, - експерт // Internetua (https://internetua.com/kiberfahivci-sbu-doveli-sxo-neperemojni-rosiiski-hakeri-ce-mif-ekspert). 13.11.2022).***

***

«Одним из сюрпризов российско-украинской войны стало то, что украинская кибербезопасность до сих пор оказывалась столь же устойчивой, как и ее вооруженные силы.

Кибертактика Киева, в том числе перенос данных в облако, партнерство с западными компаниями и использование мобильных терминалов Илона Маска Starlink для подключения к Интернету через спутник, оказалась очень эффективной.

Согласно заявлению, сделанному ранее в этом месяце, обороноспособность Украины также была подкреплена пакетом ИТ-поддержки стоимостью 6 млн фунтов стерлингов и помощью в обнаружении российских киберугроз, предоставленной Великобританией.

И, как один из самых ранних примеров конфликта с основным киберкомпонентом, эта война — и эти ответы на нее — могут послужить уроком для других стран или компаний.

В начале войны в феврале украинцы скопировали в облако как можно больше данных Затем, когда Россия вторглась в Украину, Лиам Максвелл, директор по правительственным преобразованиям в Amazon Web Services (AWS), встретился с украинским чиновником в Лондоне и «буквально записал на листе бумаги», какие цифровые активы Украины нужно было спасти. он вспоминает.

По словам Максвелла, приоритеты включали реестры собственности, граждан и преступников. «Это похоже на «иерархию потребностей» Маслоу».

Эксперты AWS по кибербезопасности и ИТ-специалисты также обучили украинцев кибербезопасности и тому, как переносить данные из локальных ИТ-систем в облако, где они могут быть лучше защищены.

В частности, они делились информацией о киберугрозах, таких как вредоносное ПО от «государственных субъектов» — из России или других стран, — которые могут затронуть клиентов AWS в Украине.

Децентрализованная сеть украинских ИТ-добровольцев, или «хактивистов», еще больше укрепила киберзащиту страны, говорит Пьерлуиджи Паганини, советник Агентства Европейского Союза по кибербезопасности.

В современной войне основной целью кибератак является уничтожение или дестабилизация критически важной национальной инфраструктуры, такой как банки, телекоммуникационные сети и энергосистемы.

Однако фрагментированный характер украинской сети связи для жизненно важных служб означает, что ее нельзя вывести из строя или заглушить так же легко, как отдельный узел, такой как вышка сотовой связи, говорят эксперты.

«В целом российские кибератаки не оказали дестабилизирующего воздействия на украинскую инфраструктуру, — отмечает Боб Коласки, бывший помощник госсекретаря, специализирующийся на кибербезопасности в Министерстве внутренней безопасности США. Сейчас Коласки является старшим вице-президентом по критической инфраструктуре в компании Exiger, которая консультирует компании по рискам. Однако Москва применила ракеты, чтобы нарушить энергетическую инфраструктуру Украины.

Хотя некоторые эксперты по безопасности удивлены тем, что кибератаки России не были более эффективными, они также хвалят тактику Украины.

Украинцы сделали «пару умных вещей», переместив данные в облако и используя Starlink для поддержания работы собственной сети связи, говорит Джеймс Льюис, старший вице-президент и директор программы стратегических технологий двухпартийного аналитического центра Center for Стратегические и международные исследования.

Льюис, который ранее консультировал ООН по информационной безопасности, подчеркивает быструю реакцию Киева на российские кибератаки.

Он говорит: «Украинцы сказали мне, что на [российскую] кибератаку нужно реагировать в течение двух-трех часов, чтобы свести к минимуму ущерб и предотвратить ее успех», — например, путем удаления вредоносных программ или уязвимостей в системе безопасности.

Украина имеет большой опыт борьбы с кибератаками.

В 2016 году хакеры отключили электричество в сотнях тысяч домов.

А в 2017 году считалось, что российские военные стоят за атакой программы-вымогателя NotPetya, нацеленной на Украину, но также зашифровавшей данные из компьютерных систем компаний в более чем 60 странах.

«Украина создала очень зрелые операции по обеспечению безопасности и реагированию на инциденты», — говорит Рэй Канзанезе, директор Netskope Threat Labs, которая исследует облачные угрозы безопасности.

С февраля большинство атак осуществлялось с помощью вредоносного программного обеспечения, известного как «вайпер», говорит Роберт Липовски, главный исследователь угроз в ESET, компании, занимающейся кибербезопасностью.

Вайпер похож на программу-вымогатель, за исключением того, что на войне цель состоит в том, чтобы уничтожить файлы, а не зашифровать их и потребовать, чтобы жертва заплатила выкуп за их возвращение.

Юрий Щеголь, глава Агентства кибербезопасности Украины, говорит, что примерно через месяц после вторжения России в Украину его агентство зарегистрировало почти в три раза больше кибератак на украинские ресурсы и инфраструктуру по сравнению с тем же периодом прошлого года.

Он говорит: «Ключевыми элементами кибер[защиты] [Украины] являются: достаточное финансирование на национальном уровне [и] в частных компаниях, управляющих критической инфраструктурой; кибергигиена на всех уровнях; и широкое международное сотрудничество».

В марте Украина присоединилась к Совместному центру передового опыта в области киберзащиты, аккредитованному НАТО учреждению, занимающемуся исследованиями в области киберзащиты.

Обмен «индикаторами угроз» и совместные учения специалистов по киберзащите имеют решающее значение, говорит Щеголь. «Это два основных аспекта системы коллективной кибербезопасности».

Россия отрицает проведение каких-либо кибератак на украинскую инфраструктуру, но ЕС, Великобритания, США и другие союзники утверждают, что она несет ответственность за ряд таких атак с начала вторжения.

По данным правительства Великобритании со ссылкой на разведданные Великобритании и США, одна такая атака в феврале привела к перебоям в работе нескольких тысяч украинских интернет-клиентов и затронула ветряные электростанции и интернет-пользователей в Центральной Европе.

По словам экспертов по кибербезопасности, Россия сама столкнулась с шквалом кибератак после вторжения в Украину.

Эксперты добавляют, что в будущем, по мере совершенствования технологий, могут появиться кибератаки и средства защиты, основанные на искусственном интеллекте.

Тем временем правительствам и компаниям рекомендуется изучить успешную украинскую тактику кибербезопасности и соответствующим образом обновить свои собственные политики безопасности.

«В киберпространстве нет мира, — предупреждает Льюис из CSIS». ***(Nick Huber. What Ukraine's cyber defence tactics can teach other nations // THE FINANCIAL TIMES LTD (https://www.ft.com/content/9635c4a0-1f42-44f1-bc9a-503b192f809f).09.11.2022).***

***

«Росія супроводжує свої ракетні удари по енергетичних об'єктах України потужними кібератаками, щоб спричинити максимальний «блекаут». Проте такі сценарії є прогнозованими, а відтак – не досягають своєї мети. Про це в інтерв'ю виданню «Ліга.НЕТ» розповів начальник Департаменту кібербезпеки СБУ Ілля Вітюк.

«СБУ постійно блокує кібератаки на об'єкти енергетики. Саме ця галузь, разом з інфраструктурою і логістикою – це пріоритетні цілі для російських спецслужб. Останні обстріли ТЕЦ та ГЕС супроводжувалися і кібератаками. В СБУ очікували на такий сценарій, тому жодна з них не була ефективною», – підкреслює Ілля Вітюк.

За його словами, в середньому рф здійснює понад 10 кібератак на Україну за добу. Більшість із них залишаються непоміченими для суспільства, але не для фахівців, які їх відбивають і локалізують.

«Ворог прагне, аби ми опинилися без світла, води, опалення, зв'язку, інтернету. Щоб люди не могли отримати інформацію, зв'язатись з близькими, не могли розплатитися у магазині… Але це вже абсолютно неможливо зараз при такому рівні нашої підготовки та реагування. У найгіршому випадку за допомогою кібератаки вони можуть, наприклад, вимкнути електроенергію на деякий час, або якісь сервіси не будуть працювати протягом нетривалого періоду, але ми працюємо, щоб навіть цього не трапилось», – наголосив Ілля Вітюк…» ***(рф щодня здійснює понад 10 кібератак на стратегічні об'єкти України, – керівник Департаменту кібербезпеки СБУ // Служба безпеки України (https://ssu.gov.ua/novyny/rf-shchodnia-zdiisniuie-ponad-10-kiberatak-na-stratehichni-obiekty-ukrainy-kerivnyk-departamentu-kiberbezpeky-sbu). 09.11.2022).***

***

«Хакери зламали Центробанк рф і отримали доступ до його мереж. Про це повідомив віцепрем'єр-міністр, міністр цифрової трансформації України Михайло Федоров.

ІТ армія отримала доступ до мереж центрального банку рф!

Дякуючи департаменту інформаційних технологій та департаменту операцій на фінансових ринках недобанку ми маємо багато цікавого про персонал, спеціалізовані автоматизовані банківські системи, їх вихідні файли, принципи їх взаємодії, системи КЗІ та інші матеріали, що церкулюють в мережах цб рф та вже аналізуються нашими фахівцями.

Глава Мінцифри виклав посилання на перші 27 тис. файлів зі зламаних мереж Центробанку рф.

Нагадаємо, після початку збройного вторгнення в Україну хакери з Anonymous оголосили війну росії». ***(Ростислав Цуркан. Хакери зламали Центробанк рф - Федоров // Подробиці (https://podrobnosti.ua/2460591-hakeri-zlamali-tsentrobank-rf-fedorov.html). 03.11.2022).***

***

«Головна ознака таких перевертнів - відсутність посилань на офіційні джерела.

Майже 20 тисяч ворожих телеграм-каналів заблокували волонтери завдяки проєкту кіберполіції «Мрія». Це телеграм-бот «Стоп Раша Мрія», з якого можна надсилати скарги адміністраторам соцмережі.

Саме телеграм-канали стали інформаційною зброєю масового ураження і своїм контентом намагаються поширити паніку серед українців. Проте і на цьому полі бою рашисти програють. Докладніше - в сюжеті Вікторії Балицької.

Оперативність та анонімність - ці дві ознаки зробили телеграм-канали ефективною зброєю у війні. Росія, у якій телеграм має найбільше користувачів, порівняно з іншими країнами світу, використовує цю соцмережу для залякування українців, пояснює кіберполіцейський Остап Кончевич. Задля цього працюють ботоферми та спецслужби. Правоохоронець ділить пропагандистські телеграм-канали рашистів на три категорії. Перша - це відверто ворожі пабліки, які працюють здебільшого на російську аудиторію.

Остап Кончевич, старший інспектор з особливих доручень Управління протидії кіберзлочинам у Львівській області:

Канали, які ведуть відверту колабораційну діяльність або є ворожими до України. Де відповідно використовується ворожа символіка, комуністична символіка, таке теж буває. Або де публічно закликають до геноциду українського народу.

Друга катеогрія - це канали, що прагнуть впливати на свідомість українців. Вони видають себе за офіційні, щоб у потрібну ворогу мить поширити дестабілізаційний вкид та ввести в оману.

Остап Кончевич, старший інспектор з особливих доручень Управління протидії кіберзлочинам у Львівській області:

Це канали, які можуть маскуватися під офіційні телеграм-канали різних військових частин, різних військових бригад, структурних підрозділів національної поліції, ДСНС.

Справжні офіційні канали завжди мають поруч із назвою так звану «галочку» і не містять реклами - пояснює поліцейський. А тексти там написані без помилок. І третя, найпопулярніша, категорія - канали, що позиціонують себе як новинні.

Остап Кончевич, старший інспектор з особливих доручень Управління протидії кіберзлочинам у Львівській області:

Вони є, я б сказав, найбільш небезпечними. Вони поширюють інформацію, так звані чутки. Вони поширюють неправдиву інформацію, неперевірену інформацію. Але тим не менше, такі канали дуже сильно розганяють паніку і дестабілізують ситуацію в певному регіоні. Насправді такі телеграм-канали можуть вестися навіть

українською мовою для того, щоб залучити більше людей особливо західних регіонів.

Головна ознака таких перевертнів - відсутність посилань на офіційні джерела. Такі телеграм-канали треба виявлити і знешкоджувати, хоч це і складно. Потрібні скарги від 60 відсотків підписників. Богдан - волонтер, який допомагає блокувати ворожі «рупори».

Нам вибиває завдання, тобто ми можемо заблокувати телеграм канал. Є пропонована скарга, ми можем її використати. Переходимо за тим посиланням на цей телеграм-канал. Ми бачимо, що він російський, він пропагандує свої новини, які є неправдивими. Ми можем нажати «поскаржитися».

Богдан - курсант вишу ДСНС, і щодня після занять він виконує свій громадянський обов’язок - заходить у телеграм-бот «Стоп Раша Мрія», щоб у такий спосіб наблизити перемогу.

Богдан Філіпчук, волонтер:

Так як я ще курсант, я теж хочу якось долучитися до війни. Наприклад, я можу сісти за комп'ютер, виконати ці пару дій і це вже буде теж якийсь маленький крок до перемоги.

Для боротьби із ворожими телеграм-каналами кіберполіція створила бот «Стоп-Раша-Мрія». З його допомогою можна надсилати скарги на ворожі публікації, які не відповідають стандартам соцмережі, та повідомляти правоохоронців про підозрілий контент. За дев’ять місяців на каналі авторизувалося понад 260 тисяч волонтерів, які усі разом зробили, здавалося, неможливе.

Валерія Івкова, старший інспектор Управління протидії кіберзлочинам у Львівській області:

Було заблоковано 19 215 телеграм каналів з активною аудиторію 230 мільйонів користувачів. Крім того, за допомогою вказаних ресурсів було додано нами до раціо, тобто на перевірку 77 тисяч ворожих посилань.

Остап Кончевич, старший інспектор з особливих доручень Управління протидії кіберзлочинам у Львівській області:

Був заблокований один з каналів, ну назви я казати не буду із зрозумілих причин, один з воєнкорів, в якого було майже 700 000 підписників. Тобто ефективність цього каналу «Мрія», вона є доведена практично.

Однак проєкт потребує ще більше волонтерів. Долучитися до «Стоп Раша Мрія» і зробити маленький крок до великої перемоги може кожен». ***(Майже 20 тисяч ворожих телеграм-каналів заблокували волонтери завдяки проєкту кіберполіції «Мрія» // Подробиці (https://podrobnosti.ua/2461450-majzhe-20-tisjach-vorozhih-telegram-kanalv-zablokuvali-volonteri-zavdjaki-proktu-kberpolts-mrja.html). 16.11.2022).***

***

«У жовтні пов'язана з російським ГРУ хакерська група атакувала логістичні організації в Україні та Польщі. Західні експерти поклали відповідальність на хакерів з угруповання Sandworm (Iridium).

Американська компанія Microsoft звинуватила російську військову розвідку у проведенні в жовтні атак програм-вимагачів, націлених на транспортні та логістичні

організації в Україні та Польщі. Конкретно відповідальність покладається на хакерське угруповання Sandworm (Iridium), ймовірно, пов'язане з російським ГРУ, повідомила в четвер, 10 листопада, американська телекомпанія CNN з посиланням на представника Microsoft.

За словами співрозмовника телекомпанії, Sandworm або Iridium використовувала для атак невідому програму-вимагач Prestige. Вона переглядала всі файли в системі комп'ютера і шифрувала вміст файлів з розширеннями.txt,.png, gpg та понад 200 інших розширень. Потім Prestige додавав розширення. enc до розширення файлу, яке існувало.

Спочатку Microsoft приписала атаку невідомій групі, яку вона назвала DEV-0960, але 10 листопада заявила, що насправді за атаками стоїть Sandworm (Iridium).

Ризики для організацій, які допомагають Україні

За допомогою програми Prestige хакери вже одержали контроль над мережами жертв. 11 жовтня хакери розгорнули Prestige на всіх заражених пристроях, зазначив співрозмовник CNN. Prestige сигналізує про підвищений ризик для організацій, які безпосередньо постачають чи транспортують гуманітарну або військову допомогу Україні. У ширшому сенсі це може становити підвищені ризики для організацій у Східній Європі, які, на думку Росії, надають підтримку Україні, додав він.

Західні країни приписують хакерській групі Sandworm або Iridium глобальну кібератаку за допомогою вірусу NotPetya у 2017 році, яка, за оцінками Білого дому, завдала фінансових збитків у розмірі 10 мільярдів доларів. Крім того, це угруповання звинувачують у зломі енергосистеми України, який викликав масові відключення електроенергії у найхолодніші місяці 2016 року та 2017 року». ***(Роман Губа, Сергій Ромашенко. Microsoft звинуватила РФ у кібератаках у Польщі та Україні // МЕДІАКОМПАНІЯ DW (https://www.dw.com/uk/microsoft-zvinuvatila-rosiu-u-kiberatakah-u-polsi-ta-ukraini/a-63726896). 11.11.2022).***

***

«Українські хакери виклади в мережу дані про співробітників ФСБ, СЗР, ГРУ та білоруського КДБ.

Як повідомляється, інформація опублікована на сайтах protozoans.net та protozoans.info, передає Цензор.НЕТ.

Публікація даних – відповідь на російський проект "Немезида". Нагадаємо, що раніше рф опублікувала дані нібито українських захисників, але в результаті більша частина із них була вигадана.

Натомість українські кіберфахівці зібрали максимально повний масив інформації: від керівництва ФСБ до звичайних оперів – телефони, дружини, кредити, паспорти, коханки.

«ProtoZoans (з лат. «одноклітинні») – аналітична система пошуку співробітників спецслужб. Усі знайдені особи причетні до військових злочинів, зовнішньої агресії, окупації та анексії територій, масових вбивств. Використовуючи аналітичну систему, ви можете знайти «одноклітинного» вбивцю, злодія та військового злочинця з ФСБ, СЗР, ГРУ і КДБ", - пишуть на сайті.

Базу даних обіцяють постійно поповнювати». ***(Телефони, коханки, кредити: хакери виклали в мережу дані співробітників російських спецслужб // Internetua***

(https://internetua.com/telefoni-kohanki-krediti-hakeri-viklali-v-mereju-dani-spivrobitnikiv-rosiiskih-specslujb). 24.11.2022).

***

«З початку повномасштабного військового вторгнення росії в Україну на об'єкти енергетичної інфраструктури було здійснено понад 1 200 000 кібератак, тоді як за весь 2021 рік їх було зафіксовано 900 000.

Про це повідомив заступник міністра енергетики з питань цифрового розвитку, цифрових трансформацій та цифровізації Фарід Сафаров, виступаючи на Energy Security Forum 2022.

Фарід Сафаров наголосив, що інтенсивні кібератаки на український енергосектор ворог почав ще до 24 лютого 2022. Так, протягом грудня 2021 та січня-лютого 2022 росіяни багаторазово намагалися здійснити втручання в роботу ключових енергетичних компаній, зламати персональні кабінети клієнтів, а також втрутитися в роботу диспетчерських центрів. Водночас високий рівень кіберзахисту українського енергосектору не дозволив рф досягнути поставлених цілей.

«Наразі росіяни продовжують намагатися «покласти» нашу енергетичну систему, застосовуючи і кібератаки, і прямі фізичні атаки ракетами та дронами. Загальна кількість кібератак за 9 місяців війни складає понад 1 200 000 випадків. Кількість DDos-атак на сайти ключових енергетичних компаній і Міністерства – більше 50, для порівняння з початку фіксації такого типу атак з 2019 року їх було тільки 5», - зазначив заступник міністра енергетики.

Фарід Сафаров наголосив на ефективній роботі кіберцентрів, які функціонують на базі НЕК «Укренерго» та НАК «Нафтогаз України». За його словами, динаміка та інтенсивність блокування тих чи інших ресурсів кіберспеціалістами збільшилася в сотні разів та за час війни досягла цифри +20 000.

Заступник міністра підкреслив, що Україна щодня набуває нового унікального досвіду у протидії кіберзагрозам, і після перемоги у війні з росією буде готова розкрити всі деталі щодо інструментарію хакерських атак, які використовує агресор». ***(З початку агресії рф зафіксовано понад 1,2 млн кібератак на енергосектор // Компьютерное Обозрение (https://ko.com.ua/z_pochatku_agresiyi_rf_zafiksovano_ponad_1_2_mln_kiberatak_na_energosektor_142673). 22.11.2022).***

***

«Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка діє при Держспецзв’язку, дослідила факти порушення цілісності та доступності інформації внаслідок застосування шкідливого програмного забезпечення «Somnia».

Відповідальність за несанкціоноване втручання в роботу автоматизованих систем та електронно-обчислювальних машин об'єкту атаки взяло на себе угруповання FRwL (aka Z-Team), активність якого відстежується CERT-UA за ідентифікатором UAC-0118.

В рамках дослідження з'ясовано, що початкова компрометація відбулася в результаті завантаження та запуску файлу, що імітував програмне забезпечення

«Advanced IP Scanner», але, насправді, містив шкідливе програмне забезпечення Vidar.

Припускається, що тактика створення копій офіційних веб-ресурсів та розповсюдження шкідливих програм під виглядом популярних програмних продуктів є прерогативою так званих брокерів початкового доступу (initial access broker). У випадку конкретно розглянутого інциденту, з огляду на очевидну приналежність викрадених даних українській організації, відповідний брокер здійснив передачу скомпрометованих даних злочинному угрупованню FRwL з метою подальшого використання для здійснення кібератаки.

Слід звернути увагу, що стілер Vidar, серед іншого, здійснює викрадення даних сесії Telegram, що, за відсутності налаштованої двохфакторної автентифікації та пасс-коду, дозволяє отримати несанкціонований доступ до облікового запису відповідної жертви.

Як було з'ясовано, Telegram жертви використовувався для передачі користувачам конфігураційних файлів VPN-підключення (в тому числі, сертифікатів та автентифікаційних даних). Зважаючи на відсутність двохфакторної автентифікації під час встановлення VPN-з'єднання, зловмисники отримали можливість несанкціонованого підключення до корпоративної мережі.

Отримавши віддалений доступ до комп'ютерної мережі організації за допомогою VPN, зловмисники провели розвідку (зокрема, застосували Netscan), виконали запуск програми Cobalt Strike Beacon, а також, здійснили ексфільтрацію даних, про що свідчить використання програми Rclone. Окрім цього, наявні ознаки запуску Anydesk та Ngrok.

З урахуванням характерних тактик, технік та кваліфікації, починаючи з весни 2022 року групою UAC-0118, за сприяння інших злочинних угруповань, причетних, зокрема, до надання початкового доступу і передачі криптованих білдів програми Cobalt Strike Beacon, проведено декілька втручань в роботу комп'ютерних мереж українських організацій.

Зауважимо, що шкідлива програма Somnia також зазнала змін. В першій версії програми використовувався симетричний алгоритм 3DES. В другій версії реалізовано алгоритм AES; при цьому, зважаючи на динамічність ключа та вектору ініціалізації, ця версія Somnia, за теоретичним задумом зловмисників, не передбачає можливості розшифрування даних». ***(Під час кібератак групи UAC-0118 використана шкідлива програма Somnia // Компьютерное Обозрение (https://ko.com.ua/pid_chas_kiberatak_grupi_uac-0118_vikoristana_shkidliva_programa_somnia_142610). 14.11.2022).***

***

Боротьба з кіберзлочинністю в Україні

«Украинская киберполиция и Европол выявили и арестовали пятерых ключевых членов международной сети мошенников, которые, по оценкам, причиняли убытки в размере более 200 миллионов евро в год.

Работа инвестиционной схемы была распространена на несколько европейских стран, включая Украину, Германию, Испанию, Латвию, Финляндию и Албанию.

Мошенники управляют колл-центрами и офисами в этих странах, чтобы обманом заставить потенциальных инвесторов инициировать серию фальшивых инвестиций.

Преступники создали обширную сеть поддельных веб-сайтов, выдающих себя за криптовалюты, акции, облигации, фьючерсы и опционные инвестиционные порталы для продвижения операции.

Эти сайты делали вид, что приносят фиктивную прибыль любым инвесторам, убеждая жертв, что они быстро зарабатывают деньги, и обманом заставляя их инвестировать еще больше.

Однако ни инвестиции, ни прибыль нельзя было вывести с платформ, и к тому времени, когда жертвы осознали мошенничество, они уже потеряли огромные суммы денег.

ФБР недавно предупредило об этом типе мошенничества, называемом «разделка свиней», предупредив общественность о том, что это очень прибыльная схема, используемая мошенниками по всему миру.

Согласно заявлению украинской киберполиции, по оценкам, преступная группировка наняла более 2000 человек в свои колл-центры, привлекая жертв на мошеннические сайты.

В Украине располагались три колл-центра, а пять человек, задержанных полицией, предположительно являются организаторами локальных операций.

«Сотрудниками правоохранительных органов были проведены обыски в домах причастных, а также по адресам колл-центров в Киеве и Ивано-Франковске», - говорится в сообщении полиции.

«Было изъято более 500 единиц компьютерной техники и мобильных телефонов».

Полицейский рейд на один из украинских колл-центров. Источник: cyberpolice.gov.ua

Украинское расследование преступной группировки ведется с 2020 года с участием Европола, Евроюста и полиции других стран ЕС.

Задержанным теперь будет предъявлено обвинение в мошенничестве по ч. 3 ст. 190 УК Украины, за которое предусмотрено наказание до восьми лет лишения свободы. ***(Bill Toulas. Ukraine arrests fraud ring members who made €200 million per year // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ukraine-arrests-fraud-ring-members-who-made-200-million-per-year/). 10.11.2022).***

***

«Кіберфахівці СБУ провели безпрецедентну спецоперацію із документування і блокування організованого злочинного угруповання, створеного громадянами рф в Україні. В результаті вдалося ліквідувати їхнє незаконне онлайн-казино, через яке у рф «пішло» близько 3 млрд у гривневому еквіваленті.

Як встановив Департамент кібербезпеки СБУ, до злочинної організації входили громадяни України та рф.

Зловмисники мали ієрархічну управлінську вертикаль, на чолі якої стояли росіяни.

Українські громадяни в угрупованні відповідали за пошук офісів та обслуговуючого персоналу, а також за рекламну підтримку, облаштування комп'ютерної техніки і авторизацію клієнтів віртуального казино. Крім того, вони моніторили платежі та налагоджували інфраструктуру, необхідну для роботи азартних ігор в мережі «Інтернет».

У результаті аналізу платіжних операцій встановлено, що за період функціонування злочинної організації з території України до рф через криптоперекази виведено майже 3 млрд грн.

Наразі співробітники Служби безпеки України повністю заблокували відповідні вебресурси, а також унеможливили доступ зловмисників до платіжних систем.

За матеріалами кібердепартаменту СБУ, десятьом організаторам і учасникам угруповання, серед яких 5 громадян України і 5 рф, повідомлено про підозру за такими статтями Кримінального кодексу України:

ч. 1, ч. 2 ст. 255 (створення, керівництво злочинною спільнотою або злочинною організацією, а також участь у ній);

ч. 2 ст. 203-2 (незаконна діяльність з організації або проведення азартних ігор, лотерей);

ч. 1, ч. 2 ст. 209 (легалізація (відмивання) майна, одержаного злочинним шляхом).

Вирішується питання щодо обрання запобіжних заходів.

Триває досудове розслідування для встановлення і притягнення до відповідальності всіх учасників злочинної організації.

Спецоперацію проводили співробітники кіберпідрозділів СБУ спільно зі слідчими Національної поліції за процесуального керівництва Київської міської прокуратури». ***(СБУ заблокувала масштабне онлайн-казино, яке «перерахувало» в рф майже 3 млрд грн // Служба безпеки України (https://ssu.gov.ua/novyny/sbu-***

zablokuvala-masshtabne-onlainkazyno-yake-pererakhuvalo-v-rf-maizhe-3-mlrd-hrn). 18.11.2022).

***

«Ресурс, що розміщувався на українському домені, пропонував платні послуги з підміни мобільних номерів. Використовуючи технологію спуфінгу, шахраї вдавали, нібито громадянам телефонують з банку і надалі отримували доступ до їхніх карток.

Організував схему громадянин Великої Британії, який наразі вже перебуває під вартою. Чоловік створив власний сайт, де пропонувався «пакет послуг» для вчинення шахрайства із використанням соціальної інженерії.

Зокрема пропонувалося здійснювати спуфінг – підміну номера телефону. У такий спосіб зловмисники могли імітувати дзвінки від банків. Роботизований голос, під різними приводами, повідомляв про необхідність надання банківських даних фейковому працівнику банку. Отримавши ці відомості, зловмисники привласнювали гроші з рахунків потерпілих. Також сервіси давали змогу перехоплювати одноразові паролі.

Коштували такі послуги від 100 до 1300 фунтів стерлінгів, в залежності від обраного «тарифу». Оплату клієнти здійснювали у криптовалюті.

Встановлено, що від протиправної діяльності ресурсу постраждали тисячі осіб, збитки сягають понад 100 мільйонів фунтів стерлінгів.

В рамках міжнародного співробітництва кіберполіція заблокувала шахрайський ресурс, який розміщувався на українському домені. У міжнародній поліцейській операції також брали участь представники Федерального Бюро розслідувань (FBI), Секретна служба США (USSS), Європол, Євроюст та правоохоронні органи Австралії, Канади, Франції, Німеччини, Ірландії, Литви та Нідерландів». ***(Кіберполіція заблокувала ресурс, який використовували іноземці для телефонного шахрайства // Офіційний сайт Кіберполіції України (https://cyberpolice.gov.ua/news/kiberpolicziya-zablokuvala-resurs-yakyj-vykorystovuvaly-inozemczi-dlya-telefonnogo-shaxrajstva-7936/). 24.11.2022).***

***

«Використовуючи фішингові посилання, зловмисники привласнили понад 400 тисяч гривень. За скоєне їм може загрожувати до восьми років позбавлення волі.

Протиправну діяльність чотирьох жителів Павлограда викрили працівники управління протидії кіберзлочинам в Дніпропетровській області спільно зі слідчими Дніпровського районного управління поліції та у співпраці зі службою безпеки ПриватБанку.

Фігуранти знаходили оголошення щодо продажу товарів на тематичних платформах та для обговорення деталей писали продавцям у сторонні месенджери. Туди зловмисники надсилали фішингові посилання нібито про інтернет-оплату. Коли продавці переходили за посиланням та вводили дані банківської карти, ці відомості одразу ставали відомі шахраям.

Отримавши доступ до банківських рахунків, зловмисники переводили гроші потерпілих на підконтрольні картки, оформлені на третіх осіб. Встановлено, що у такий спосіб вони привласнили понад 400 тисяч гривень.

За місцями проживання фігурантів правоохоронці провели обшуки: вилучено комп'ютерну техніку, мобільні телефони, флеш-носії та банківські картки.

Відкрито кримінальне провадження за ч. 3 ст. 190 (Шахрайство), ч. 2 ст. 361 (Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж) Кримінального кодексу України. Одному з фігурантів уже повідомлено про підозру». ***(У Дніпрі кіберполіція викрила зловмисників у шахрайстві з використанням фішингу на платформі оголошень // Офіційний сайт Кіберполіції України (https://cyberpolice.gov.ua/news/u-dnipri-kiberpolicziya-vykryla-zlovmysnykiv-u-shaxrajstvi-z-vykorystannyam-fishyngu-na-platformi-ogoloshen-260/). 22.11.2022).***

***

«…Співробітники Департаменту кіберполіції спільно з Головним слідчим управлінням Нацполіції, Офісом Генерального прокурора, представниками Європолу, Євроюсту викрили п'ятьох громадян України, які є учасниками масштабної міжнародної злочинної схеми. Документування дій зловмисників відбувалося у взаємодії з правоохоронцями Албанії, Фінляндії, Грузії, Німеччини, Латвії та Іспанії. Розслідування кібершахрайства розпочалося у 2020 році, зокрема і в Україні. Наразі сім країн порушили судові справи за даним фактом.

Зловмисники мали власні вебресурси, на яких пропонували вкладникам отримання надприбутків від інвестування у криптовалюту, торгівлі цінними паперами (акції, облігації, ф'ючерси, опціони). На платформах імітувалося зростання активів, однак інвестори не мали змоги перевести «зароблене» у готівку.

Для переконання потенційних вкладників зловмисники утворили call-центри у кількох країнах Європи. Там працювало понад 2 тисячі осіб. На території України діяло три таких call-центри, п'ятеро фігурантів відповідали за організацію їхньої роботи.

За даними Європолу, від протиправної діяльності транснаціонального угруповання постраждали сотні тисяч осіб по всьому світу. Збитки оцінюються у понад 200 мільйонів євро на рік.

В оселях фігурантів, а також за адресами розташування call-центрів, у Києві та Івано-Франківську, правоохоронці провели обшуки. Вилучено понад 500 одиниць комп'ютерної техніки, мобільні телефони. Одночасно обшуки проходили в інших країнах за місцями проживання решти учасників групи.

Відкрито кримінальне провадження за ч. 3 ст. 190 (Шахрайство) Кримінального кодексу України. Санкція статті передбачає до восьми років позбавлення волі». ***(Кіберполіція викрила учасників транснаціональної шахрайської групи у привласненні грошей сотень тисяч осіб по всьому світу // Офіційний сайт Кіберполіції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-uchasnykiv-***

transnaczionalnoyi-shaxrajskoyi-grupy-u-pryvlasnenni-groshej-soten-tysyach-osib-po-vsomu-svitu-4457/). 10.11.2022).

***

«Протиправну схему фігуранти налагодили з метою заробітку. Вони створювали штучне навантаження на електронні системи, відтак унеможливлювали реєстрацію користувачів в електронній черзі для отримання документів за кордоном. Щонайменше 150 громадян України вимушено скористалися платними послугами фігурантів для отримання талонів у черзі.

Правопорушників викрили працівники Департаменту кіберполіції спільно зі слідчими Печерського управління поліції Києва та за сприяння Державної міграційної служби України.

Організувала схему 43-річна мешканка Сумської області, яка залучила ще чотирьох знайомих.

Фігуранти за допомогою великої кількості зовнішніх запитів створювали навантаження на системи ДП «Документ» у Польщі. У такий спосіб вони перешкоджали іншим користувачам отримати електронні талони у черзі для оформлення документів. Паралельно зловмисники розміщували рекламу у соцмережах та месенджерах щодо «місця у черзі». Коштувала така послуга 800-1500 гривень.

За попередніми даними, протиправна діяльність групи тривала з червня 2022 року. Встановлено, що за цей час понад 150 громадян України вимушено скористалися платними послугами зловмисників. Наразі правоохоронці встановлюють остаточну кількість потерпілих.

В оселях фігурантів та за адресами вчинення протиправних дій правоохоронці провели обшуки. Вилучено комп'ютерну техніку та мобільні телефони, які використовувалися для реалізації схеми. Вилучене направлено на проведення комп’ютерно-технічних експертиз.

Відкрито кримінальне провадження за ч. 5 ст. 361 (Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, вчинені під час дії воєнного стану) Кримінального кодексу України. За скоєне зловмисникам може загрожувати до п’ятнадцяти років позбавлення волі. Вирішується питання щодо оголошення підозри.

Процесуальне керівництво здійснює Печерська окружна прокуратура». ***(Кіберполіція викрила зловмисників у несанкціонованому втручанні в електронні системи державної установи з виготовлення українських документів // Офіційний сайт Кіберполіції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-zlovmysnykiv-u-nesankczionovanomu-vtruchanni-v-elektronni-systemy-derzhavnoyi-ustanovy-z-vygotovlennya-ukrayinskyx-dokumentiv-1303/). 08.11.2022).***

***

«Фігурантка ошукала більше 120 громадян під виглядом продажу автівок в інтернеті. Від потенційних покупців вона отримувала завдаток, а потім «зникала». За скоєне їй може загрожувати до восьми років за ґратами.

Схему онлайн-шахрайства викрили співробітники відділу протидії кіберзлочинам у Миколаївській області спільно зі слідчими Первомайського районного відділу поліції.

Зловмисниця, мешканка Одеської області, на торговельних майданчиках розміщувала фейкові оголошення про продаж автомобілів. Фігурантка «пропонувала» лише ті автівки, що мають попит та можуть використовуватися для потреб військових.

Від охочих придбати авто жінка отримувала передплату на рахунки, оформлені на підставних осіб. Однак взятих на себе обов'язків не виконувала, оголошення видаляла та припиняла зв'язок із клієнтами.

За попередніми підрахунками, у такий спосіб вона привласнила гроші близько 120 громадян. Серед ошуканих – військовослужбовці ЗСУ та волонтери. Сума збитків наразі встановлюється.

В оселі зловмисниці правоохоронці провели санкціонований обшук. За результатами вилучено комп'ютерну техніку та 16 мобільних телефонів, а також банківські картки та понад три десятки SIM-карток різних мобільних операторів. Вилучене направлено на проведення експертних досліджень.

Відкрито кримінальне провадження за ч. 3 ст. 190 (Шахрайство) Кримінального кодексу України. Санкція статті передбачає до восьми років позбавлення волі. Вирішується питання щодо повідомлення фігурантці про підозру.

Процесуальне керівництво здійснює Кривоозерський відділ Первомайської окружної прокуратури Миколаївської області». ***(Кіберполіцейські Миколаївщини викрили зловмисницю у привласненні грошей військових та волонтерів // Офіційний сайт Кіберполіції України (https://cyberpolice.gov.ua/news/kiberpoliczejski-mykolayivshhyny-vykryly-zlovmysnyczyu-u-pryvlasnenni-groshej-vijskovyx-ta-volonteriv-6851/). 04.11.2022).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Официальные лица США и Италии созвали конференцию Cyber Defense Pledge Conference 2022, посвященную поддержке Украины и инвестированию в новые технологии для всех стран-членов.

Официальные представители правительств США и Италии собрались в четверг в Риме, ознаменовав начало конференции Организации Североатлантического договора по обеспечению киберзащиты 2022 года, основной целью встречи было сохранение единого фронта в условиях продолжающихся боевых действий между Россией и Украиной.

Заместитель министра иностранных дел Италии Эдмондо Чириелли открыл саммит, обсудив, как правительства стран-членов планируют модернизировать

операции военного времени, в частности, обновляя киберпространство новыми технологиями, чтобы лучше соответствовать технологическим достижениям в войне.

В этом году особое внимание уделяется «Устойчивости, готовности и реагированию на киберугрозы критически важной инфраструктуре». устойчивость.

«Конфликт в Украине — это война на истощение, напоминающая нам о Первой мировой войне, но в то же время являющаяся примером поля боя 21 века», — сказал Чириелли. «Мы видим окопы, но мы также видим взлом… чтобы нарушить украинскую военную связь».

Чириелли сослался на искусственный интеллект, особенно с целью большей автоматизации, как на приоритет для внедрения в боевых операциях.

Энн Нойбергер, заместитель советника по национальной безопасности по кибербезопасности и новым технологиям в Совете национальной безопасности, согласилась с Сириелли в своем вступительном слове. Она удвоила приверженность НАТО внедрению более надежных протоколов кибербезопасности в отдельных цифровых системах группы.

«Национальные лидеры и эксперты в области кибербезопасности созовут группы, чтобы сосредоточиться на защите энергетического сектора от киберугроз и обеспечении того, чтобы обязательство НАТО по киберзащите идти в ногу с меняющимся ландшафтом киберугроз», — сообщил Nextgov представитель Госдепартамента.

Нойбергер подчеркнул предыдущие инициативы НАТО, разработанные на летней встрече в Мадриде, сославшись на новую структуру Стратегической концепции НАТО, которую страны-союзники примут для создания более надежной киберзащиты в критически важных инфраструктурах.

«Мы развиваем национальные кибервозможности, чтобы мы как альянс были в большей безопасности», — прокомментировала она. «Мы все несем ответственность за создание национальной киберзащиты». Частью этого обещания является работа над тем, чтобы действовать быстрее, чтобы оказывать «гибкую» техническую и политическую поддержку другим странам НАТО.

Генеральный секретарь НАТО Йенс Столтенберг был третьим спикером на вступительном протоколе встречи, чтобы подчеркнуть характер «невидимой войны в киберпространстве», и пообещал постоянную поддержку Украины, поскольку Россия ведет цифровую войну.

«Благодаря мощной поддержке НАТО мы годами работали над усилением киберзащиты Украины, проводя обучение и обмениваясь информацией и разведданными», — сказал он. «Кибер — это постоянно оспариваемое пространство, и грань между миром, кризисом и конфликтом стирается».

Столтенберг также отметил, что НАТО признает, что кибератаки подпадают под действие пятой статьи НАТО, которая определяет нападение на одно государство-член как нападение на всех.

«Кибер теперь является областью операций, равной той, что на суше, на море, в воздухе и в космосе», — подтвердил он.

Он продолжил говорить, что НАТО проводит регулярные учения по киберзащите, и выделил обе принимающие страны — Италию и США — как

союзников с надежной киберзащитой, в частности сославшись на недавний закон президента Джо Байдена, направленный на более эффективный мониторинг атак программ-вымогателей.

Частные компании также пришли на помощь странам НАТО. Столтенберг отметил, что облачное программное обеспечение Microsoft и Amazon обеспечивает безопасное убежище для министерских данных Украины, поскольку Россия работала над взломом ее правительственных сетей. Он также сослался на то, что YouTube и другие социальные сети занимают более строгую позицию по модерации контента на русском языке.

«Угроза из киберпространства реальна, и она растет», — заключил Столтенберг. «Вот почему наше обязательство по киберзащите так важно. Поэтому я призываю союзников возобновить киберзащиту с большими инвестициями, большим опытом и расширенным сотрудничеством». ***(Alexandra Kelley. NATO Allies Double Down on Cybersecurity in Warfighting Ops // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/nato-allies-double-down-cybersecurity-warfighting-ops/379618/). 10.11.2022).***

***

«Корпорація Microsoft подовжує підтримку України до кінця 2023 року і надасть технологічну допомогу ще на 100 млн дол. Про це повідомив віце-президент компанії Бред Сміт під час зустрічі з Михайлом Федоровим, міністром цифрової трансформації України.

Технічна допомога дасть змогу державним установам, критичній інфраструктурі та іншим секторам в Україні продовжувати безоплатно використовувати цифрову інфраструктуру та працювати в хмарі Microsoft.

З початку повномасштабної війни сумарна допомога Microsoft вже перевищила 400 млн дол. Крім надання можливості користуватися її хмарними сервісами компанія продовжує підтримувати нашу країну у сфері критично важливої кібербезпеки; підтримувати некомерційні та гуманітарні організації; надає дані та підтримує міжнародні організації, що допомагають Україні та розглядають воєнні злочини проти цивільного населення тощо.

«З початком повномасштабної війни Microsoft надала Україні технології, які зіграли вирішальну роль у захисті стійкості та безпеки даних громадян. Корпорація вже надала безоплатні хмарні сервіси на 2022 рік, а тепер продовжила термін до кінця 2023 року. Також оголосила про нову технологічну допомогу, яка дасть змогу оцифрувати якомога більше державних відомств, зокрема підтримати реформу Державної служби статистики», – зазначив Федоров.

Крім того, компанія стала однією з перших, яка ще на початку березня призупинила всі нові продажі продуктів і послуг у росії». ***(Microsoft подовжує технічну допомогу Україні ще на рік та виділяє на це 100 млн дол. // Компьютерное Обозрение (https://ko.com.ua/microsoft_podovzhuye_tehnichnu_dopomogu_ukrayini_shhe_na_rik_ta_vidilyaye_na_ce_100_mln_dol_142525). 04.11.2022).***

***

«Правительство Великобритании сообщило, что Великобритания тратит миллионы фунтов стерлингов на усиление киберзащиты Украины, защиту критической инфраструктуры страны и государственных служб от злонамеренных атак.

В ответ на рост «темпа» российской киберактивности после вторжения президента Владимира Путина в феврале был введен первоначальный пакет в размере 6,35 млн фунтов стерлингов (7,2 млн долларов США).

Но до сих пор об этом молчали из соображений безопасности, заявили в правительстве.

Это произошло после того, как Национальный центр кибербезопасности, входящий в состав разведывательной организации GCHQ, опубликовал свой ежегодный обзор, обнаружив, что угроза кибербезопасности для Великобритании «значительно возросла» за последний год: 18 инцидентов с программами-вымогателями требуют координации на национальном уровне. отклик.

Среди них нападения на поставщика Национальной службы здравоохранения и водоканал.

До сих пор украинская схема обеспечивала поддержку реагирования на инциденты, помогала укрепить критическую инфраструктуру от будущих атак и предоставляла передовые системы кибербезопасности, включая брандмауэры и средства судебной экспертизы, чтобы предложить дополнительный уровень защиты и понимания.

Министр иностранных дел Джеймс Клеверли предупредил, что нападение России на Украину «не ограничивается ее ужасающим вторжением на территорию», поскольку Москва «настойчиво пытается вторгнуться в киберпространство Украины, угрожая критически важной информации, услугам и инфраструктуре».

Правительство заявило, что российские субъекты имеют «долгую историю враждебной и дестабилизирующей деятельности» против Украины, а прошлые цели, как утверждалось, включали электросеть страны, финансовый и энергетический секторы, а также киевское метро и аэропорт Одессы.

NCSC ранее заявлял, что имеет «высокую уверенность» в том, что за некоторыми из этих атак, в том числе за нарушением работы транспортной системы, «почти наверняка» стоит российская военная разведка ГРУ.

Ранее Москва отрицала свою причастность к кибератакам на Украине.

«Поддержка Великобританией Украины не ограничивается военной помощью, — сказал г-н Клеверли. — Мы используем передовой британский опыт для поддержки киберзащиты Украины.

«Вместе мы обеспечим поражение Кремля во всех сферах: на земле, в воздухе и в киберпространстве».

Исполнительный директор NCSC Линди Кэмерон сказала: «NCSC гордится тем, что сыграла свою роль в поддержке украинских киберзащитников…» ***(Soraya Ebrahimi. UK spends millions strengthening Ukraine's cyber security // The National (https://www.thenationalnews.com/world/uk-news/2022/11/01/uk-spends-millions-strengthening-ukraines-cyber-security/). 02.11.2022).***

***

«Правительство Германии выделит дополнительно 1 млрд евро из бюджета на 2023 год для поддержки Украины. Средства пойдут, в частности, на защиту от российских кибератак и сбор доказательств в связи с военными преступлениями. Об этом говорится в постановлении, выдержки из которого в пятницу, 11 ноября, привело агентство Reuters.

Часть финансирования будет перечислена группам специалистов, фиксирующих свидетельства нарушений прав человека и военных преступлений, в том числе после вывода войск РФ из ранее оккупированных областей Украины.

Дополнительные средства будут направлены на поддержку гражданского общества в регионе, включая защиту журналистов в Беларуси, России и Украине.

«Мы инвестируем в мир в Европе и Украине»

Выделение финансов происходит на фоне споров о том, должна ли Германия увеличить объем военной помощи Украине. Решение о направлении средств принято под давлением «Союза-90»/«зеленых».

«Украинский бюджет ясно показывает, что наша поддержка выходит далеко за рамки важных и необходимых поставок оружия», - отметил депутат германского бундестага от «зеленых» Робин Вагенер (Robin Wagener), возглавляющий парламентскую группу по Украине. «Мы инвестируем значительные средства в мир в Европе и Украине», - добавил он.

Германия является третьим по величине военным донором Украины после США и Канады.

Германо-украинский форум под девизом Rebuild Ukraine

Ранее, 24 октября, по итогам прошедшего в Берлине под девизом «Rebuild Ukraine» («Восстановить Украину») 5-го Германо-украинского бизнес-форума канцлер ФРГ Олаф Шольц (Olaf Scholz), обращаясь к немецким деловым кругам, подчеркнул: «Тот, кто сегодня инвестирует в восстановление Украины, тот инвестирует в страну - будущего члена ЕС, которая станет частью нашего правового пространства и нашего внутреннего рынка».

Приехавший в Берлин премьер-министр Украины Денис Шмыгаль выразил уверенность, что восстановление его страны станет бустером для экономики ЕС, катализатором ее развития. Он заверил, что правительство в Киеве взяло курс на стимулирование частной инициативы, на дерегулирование бизнеса, на снижение роли государства в деловой жизни.

Среди самых перспективных направлений будущего сотрудничества он назвал оборонную промышленность, энергетику (с упором, в частности, на газовую сферу), IT-индустрию и цифровизацию, сельское хозяйство, а также разработку и внедрение экологически чистых технологий в рамках европейского «зеленого» курса, получившего название Green Deal». ***(Екатерина Венкина. ФРГ выделит 1 млрд евро на кибербезопасность Украины // Deutsche Welle (https://www.dw.com/ru/frg-vydelit-1-mlrd-evro-na-kiberbezopasnost-ukrainy-i-sbor-dokazatelstv-voennyh-prestuplenij-rf/a-63733750). 11.11.2022).***

***

«Новое исследование, проведенное австралийской некоммерческой инициативой по поддержке психического здоровья в киберпространстве, Cybermindz.org демонстрирует ранние свидетельства эмоционального выгорания киберспециалистов, сигнализирующие о потенциальной потере навыков в критической части экономики.

Организация быстро признает, что стресс и выгорание не уникальны для кибербезопасности, но указывает, что системные недостатки в нашей киберзащите человека будут иметь тенденцию влиять на общество на массовом уровне, особенно если основные услуги, такие как вода, энергия, телекоммуникации, здравоохранение, финансы затронуты услуги, распределение продуктов питания и транспорт.

По мере того, как страна переваривает продолжающиеся последствия взломов Optus, Medibank и MyDeal, а также других, которые становятся известны, организация предупредила, что, если политики не признают воздействия на психическое здоровье австралийской рабочей силы в киберпространстве, ухудшение психического здоровья основных защитники могут ускориться, создавая каскадный эффект снижения эффективности и повышения риска.

Хотя исследование продолжается и продлится до конца года, основатель Cybermindz и опытный лидер интернет-индустрии Питер Коронеос объяснил важность сигнализирования о зарождающейся тенденции, сравнив ее с «канарейкой в угольной шахте кибербезопасности».

Он заметил: «Большинство наших критически важных систем в настоящее время подвержены киберрискам — нетрудно понять, что снижение наших национальных кибервозможностей из-за психологического выгорания может иметь последующие последствия для всего населения. Пандемия, наводнения и лесные пожары показали нам, что системы, на которые мы полагаемся, не следует воспринимать как нечто само собой разумеющееся. Кибератаки — повседневное явление, и, в отличие от стихийных бедствий, в поле зрения нет никакой мыслимой конечной точки».

Г-н Коронеос добавил: «Работники кибербезопасности — незамеченные герои нашего времени. Их повседневная работа невидима, но один сбой из-за взлома, который может затронуть миллионы людей, попадает в заголовки. Быстро развивающаяся и безжалостная среда атак бросает вызов любому чувству «хорошо выполненной работы». Одна успешная атака, которая может положить конец их карьере, может быть не за горами. Они ориентированы на миссию с сильным защитным духом. Но чувство безнадежности в конечном итоге сказывается даже на самом преданном работнике. Поэтому важно, чтобы мы признавали их усилия и инвестировали в их благополучие. Мы должны создать сильную и устойчивую рабочую силу в области кибербезопасности. Если они упадут, упадем мы все».

Исследование возглавляет директор отдела организационных и поведенческих исследований Cybermindz.org доктор Эндрю Ривз.

Доктор Ривз заявил: «Хотя это предварительные результаты, они указывают на тревожную тенденцию. По ключевому показателю выгорания «профессиональная

эффективность» — или насколько хорошо, по мнению кибер-работников, они справляются со своими текущими ролями — они показали значительно худшие результаты, чем население в целом. Мы также сравнили уровень их выгорания по этому показателю с показателями другой сильно выгоревшей отрасли: передовых медицинских работников, и обнаружили, что киберпрофессионалы набирают значительно более низкие баллы по этому показателю, чем даже представители этой группы.

Доктор Ривз добавил: «Это вызывает беспокойство, поскольку этот показатель является показателем намерения уйти в отставку. В результате, я думаю, мы видим ранние признаки того, что группа профессионалов сомневается в собственной эффективности и приходит к выводу, что их усилия напрасны. Когда хорошие люди уходят из отрасли, мы теряем так много знаний и опыта. Затем это увеличивает давление на тех, кто остается позади. Мы все должны быть обеспокоены психологическим фактором выгорания». ***(Cybersecurity Professionals May Be Burning Out at a Faster Rate Than Frontline Healthcare Workers // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/international-counter-ransomware-initiative-2022-joint-statement/). 01.11.2022).***

***

«Кибератаки, нацеленные на физическую инфраструктуру, могут иметь разрушительные физические последствия, помимо нарушения работы.

«Конвергенция безопасности» — это отраслевой термин, используемый для описания объединения кибербезопасности и физической безопасности в единую организационную структуру. Это является предметом обсуждения среди практиков с тех пор, как ASIS International и Ассоциация аудита и контроля информационных систем (ISACA) 17 лет назад создали Альянс по управлению рисками безопасности предприятия – организацию, занимающуюся этой концепцией. Тем не менее, только 52,5 процента опрошенных крупных компаний «полностью или частично конвергентны», как отмечает Меган Гейтс в последнем выпуске Security Management.. Гейтс также ссылается на инцидент с Colonial Pipeline, который работал как традиционно разрозненная программа кибер- и физической безопасности, а теперь объединяет функции безопасности после того, как в мае произошла мощная атака программы-вымогателя. Поставщики критической инфраструктуры, особенно в энергетическом секторе, не могут эффективно работать с информационными хранилищами кибер- и физической безопасности.

В условиях быстро меняющихся геополитических рисков, постоянных киберугроз, продолжающегося распространения COVID-19 с сезонными горячими точками, а также насильственных кинетических атак и конфликтов, происходящих по всему миру, компании переосмыслили традиционные системы управления рисками предприятия, чтобы учесть все риски и опасности. Поверхность рисков для поставщиков критической инфраструктуры, особенно в энергетическом секторе, сложна.

Во-первых, поставщики энергии, работающие в динамичном мире рассредоточенных операций по производству, распределению и передаче, часто имеют обширную инфраструктуру, расположенную во всех типах опасных сред —

от городских до изолированных сельских районов. Например, эти подстанции крупных электрических систем или важные трубопроводы подпадают под различное нормативное регулирование (включая директивы NERC/CIP, CFATS и TSA по безопасности трубопроводов), большинство из которых требует надежной кибербезопасности и даже контроля физической безопасности (например, NERC/CIP 14). Во-вторых, поставщики энергии становятся все более уязвимыми для атак с использованием операционных технологий — кибератак, нацеленных на физическую инфраструктуру и могущих иметь разрушительные физические последствия, помимо нарушения работы.

Кроме того, изощренные кибератаки на сеть все чаще используются государственными субъектами для того, чтобы наказать противников неатрибуционным или запутанным способом. Ранее в этом году DHS даже предупредил о том, что местные воинствующие экстремисты атакуют инфраструктуру для физического нападения, чтобы создать повсеместный хаос и подорвать доверие к правительству. В сентябре газопровод Nord Stream подвергся саботажу по дну Балтийского моря.— яркое напоминание о том, что хирургическая атака может нанести ущерб незащищенной инфраструктуре. Глобальная геополитическая нестабильность только увеличила вероятность конвергентной атаки, в ходе которой изощренный злоумышленник получает доступ к критически важному объекту или местоположению и внедряет вредоносное ПО непосредственно в системы АСУ ТП/SCADA. Системы /OT могут предотвратить. Хуже того, скоординированная кибер- и физическая атака, направленная одновременно на разрозненные ключевые узлы электрической системы, может иметь усиливающий и каскадный эффект.

Основываясь на этих угрозах, регулирующие органы пытаются добиться большей конвергенции безопасности и физической и кибер-координации в энергетическом секторе. В дополнение к изложению требований физической безопасности последняя Директива TSA по безопасности трубопроводов, выпущенная в июле, требует, чтобы охваченные «владельцы / операторы» «имели актуальный план реагирования на инциденты кибербезопасности, который включает меры по снижению риска нарушения работы». В дополнение к базовым критериям кибербезопасности, NERC CIP-014-1 Физическая безопасностьтакже требует, чтобы операторы передачи «идентифицировали и защищали передающие станции и передающие подстанции, а также связанные с ними первичные центры управления, которые, если они будут выведены из строя или повреждены в результате физической атаки, могут привести к широко распространенной нестабильности, неконтролируемому разделению или каскадированию внутри соединения.»

Центр обмена и анализа информации об электроэнергетике NERC (E-ISAC) также два раза в год возглавляет учения GridEx, чтобы предложить «членам и партнерским организациям форум для практики, как они будут реагировать и восстанавливаться после скоординированных угроз и инцидентов кибер- и физической безопасности». Планировщики GridEx продолжают предвидеть рост изощренных, скоординированных атак, которые бросят вызов традиционно разрозненным организациям по обеспечению безопасности. При целостном

прочтении эти ключевые режимы регулирования и учений подчеркивают совпадающие кибер- и физические риски.

Критичность сектора, его зависимость от децентрализованной, незащищенной инфраструктуры, а также изобретательность и изощренность противников требуют демонтажа информационных бункеров в организациях безопасности. Лучший способ устранить разрозненность — объединить функции безопасности под руководством одного подотчетного руководителя, ответственного за решения и инвестиции в области управления рисками, связанными с безопасностью. В инкрементной модели программы физической безопасности будут объединяться с функциями безопасности ОТ (вместо всей экосистемы кибербезопасности ИТ), объединяя в единой цепочке управления критически важные функции, которые предотвращают гибридные угрозы и атаки, реагируют на них и восстанавливаются.

Для управления этими непредвиденными обстоятельствами безопасности с «хвостовым риском» или рисками с низкой вероятностью и большими последствиями объединенная или специализированная межфункциональная группа может:

Учтите объединенную рабочую группу по угрозам в организации по безопасности, которая собирается регулярно или в ответ на оперативную или предполагаемую угрозу компании. Обеспечьте обмен информацией и рекомендациями экспертов по ОТ/кибербезопасности и физической безопасности для подготовки к атакам, реагирования на них и восстановления после них.

Разработайте внутреннюю функцию анализа рисков. Эта единая команда отвечает за сбор, анализ и распространение информации о кибер- и физических угрозах и рисках. Работайте с группой исполнительного руководства и руководителями оперативных подразделений (например, с руководителями генерирующих или передающих) для разработки оперативных приоритетов разведки. Обобщайте информацию от правительства и инициатив по обмену информацией и продолжайте совершенствовать бюллетени об угрозах.

Внедрите проверку мер безопасности и процедур с учетом угроз. Разрабатывайте и постоянно обновляйте объединенный набор тактик, методов и процедур противника («TTP»), т. е. проектную угрозу, отражающую реальные и правдоподобные действия противника. Оцените существующие меры безопасности по отношению к этому ранжированному по степени риска списку векторов угроз и разработайте соответствующие стандарты проектирования, которые лучше всего обнаруживают, задерживают и устраняют гибридные угрозы.

Конвергенция — это не панацея, подходящая для каждой компании и любого сектора. Специалисты по кибербезопасности и физической безопасности обладают специализированными наборами навыков и опытом, которые со временем развивались и требуют постоянной специализации. Каждый из них предлагает уникальные точки зрения, которые могут пролить свет на то, как злоумышленник может использовать уязвимость. Однако у поставщиков критической инфраструктуры, особенно в энергетическом секторе, отсутствуют встроенные средства защиты, предоставляемые другим отраслям (например, совместное размещение ценных активов или систем, менее постоянная активность угроз и ограниченное физическое воздействие от атаки). Вместо этого эти организации

становятся мишенью для изощренных злоумышленников, управляют обширными массивами незащищенной инфраструктуры с присущими ей физическими и кибер-уязвимостями и предоставляют услуги, которые напрямую влияют на способность общества функционировать». ***(Ben Joelson. Cyber and Physical Threats Illuminate Need for Security Convergence in Energy Sector (https://www.hstoday.us/featured/cyber-and-physical-threats-illuminate-need-for-security-convergence-in-energy-sector/). 29.11.2022).***

***

«Отчет о кибербезопасности SANS OT/ICS за 2022 год показывает, что хакеры по-прежнему проявляют очень большой интерес к промышленным системам управления, но организации, как правило, гораздо лучше подготовлены после громких инцидентов 2021 года. Это по-прежнему не является универсальной тенденцией, однако, поскольку 35 % до сих пор не могут определить, были ли они скомпрометированы, а 17 % до сих пор не следят за безопасностью системы OT.

Опрос проводится лидером в области кибербезопасности Nozomi Networks и Институтом SANS, ведущим исследовательским и учебным центром. Он включает в себя вклад более 330 менеджеров, аналитиков и архитекторов безопасности, занимающихся кибербезопасностью ICS, представляющих фирмы со всего мира.

Осведомленность о кибербезопасности АСУ растет вместе с атаками, но некоторые организации продолжают бороться

2021 год стал важным тревожным звонком для кибербезопасности АСУ ТП, поскольку криминальные группы программ-вымогателей перешли черту и атаковали критически важные системы инфраструктуры и пытались нанести физический реальный ущерб, наиболее известными из которых были разрушительные атаки на Colonial Pipeline и гиганта по упаковке мяса JBS.

Отчет о кибербезопасности ICS за 2022 год определенно показывает, что отрасль реагирует на эти инциденты, демонстрируя лучшую готовность и большую готовность выделять средства на кибербезопасность ICS в целом. Тем не менее, все еще существует значительное количество уязвимых организаций, которым предстоит столкнуться с серьезными проблемами, чтобы справиться с ландшафтом угроз.

В настоящее время большинство организаций признают угрозы АСУ очень серьезными; 22% оценили их как «критические», а 41% оценили их как «высокоприоритетные», что представляет собой медленный, но неуклонный рост за последние несколько лет. Опрос также указывает на растущее осознание того, что миры стандартной ИТ-безопасности и кибербезопасности АСУ ТП существенно различаются и требуют разных наборов навыков, поскольку 80 % специалистов по безопасности заявили, что теперь их роль делает упор на АСУ ТП (по сравнению с 50 % в предыдущий год). Большинство респондентов, которые делили свое время между ICS и бизнес-ролью, также говорят, что ICS теперь имеет приоритет.

Респонденты также рассказали о своих самых больших индивидуальных проблемах кибербезопасности АСУ ТП. Неудивительно, что главной проблемой была интеграция устаревших устаревших систем с современными ИТ-сетями. Это

была хроническая проблема, поскольку промышленное оборудование, как правило, рассчитано на десятилетия, а также совсем недавно начало предвидеть интернет-угрозы. Но не отставала и озабоченность тем, что современные ИТ-системы все еще не приспособлены для взаимодействия с промышленным оборудованием и системами управления. Другие серьезные проблемы включают нехватку ИТ-персонала, понимающего эксплуатационные требования ОТ, и нехватку рабочей силы для реализации существующих планов обеспечения безопасности.

С точки зрения бизнеса главной заботой является способность обеспечить надежность и доступность систем управления. Другими важными проблемами являются снижение риска при одновременном повышении безопасности, предотвращении повреждения систем, предотвращении утечки информации и соблюдении нормативных требований.

Бюджеты также выросли: только 7% сообщили, что у них нет никакого бюджета на кибербезопасность АСУ ТП (по сравнению с 21% в предыдущем году), и организации обычно увеличивают свои бюджеты в этой области на сотни тысяч долларов.

Бад Брумхед (Bud Broomhead) (генеральный директор Viakoo) полагает, что те, кто по-прежнему не решается вкладывать средства в эту область, скоро приложат все усилия: «Рост программ-вымогателей и других атак на инфраструктуру ОТ напрямую приведет к тому, что организациям потребуется больше данных и информации. в своих ОТ-системах для получения страховки кибербезопасности. Даже при таком страховании кибербезопасности среды ОТ и IOT будут стоить значительно дороже из-за этих угроз. Организациям необходимо начать свой путь к безопасности, особенно с ОТ. Это начинается с обнаружения активов, за которыми следуют автоматизированные методы исправления».

Восприятие риска зависит от отрасли, некоторые организации отстают

Некоторые секторы подвергаются гораздо большему риску компрометации, чем другие, по крайней мере, судя по тому, как респонденты оценивают вероятность компрометации в своей области. Группами, которые считаются наиболее подверженными риску, являются бизнес-услуги, здравоохранение/общественное здравоохранение, коммерческие объекты, финансовые услуги и критическое производство. Сектора, которые, по мнению респондентов, представляют наименьший риск, относятся к числу тех, которые подвергаются серьезному нападению, но также и надежно защищены: плотины, атомные станции, аварийно-спасательные службы и химические компании.

Также считается, что некоторые компоненты представляют гораздо более высокий риск, чем другие. Респонденты ожидают, что инженерные элементы, активы оператора и серверные активы с большей вероятностью будут скомпрометированы, чем что-либо еще. Это также компоненты, которые респонденты оценили как имеющие наибольшее негативное влияние в случае их взлома.

Хотя осведомленность в целом повышается из-за череды атак программ-вымогателей на критически важную инфраструктуру, некоторые организации по-прежнему отстают от кибербезопасности АСУ ТП. В целом чуть менее половины респондентов используют активное сканирование уязвимостей в этой области, а

36,5% просто ждут, пока поставщики уведомят их о проблеме или пришлют исправление. Только 34,5% говорят, что активно ищут уведомления об уязвимостях по мере их поступления.

Эндрю Барратт, вице-президент Coalfire, раскрывает важность активного мониторинга в этой области: «Атака на среды OT часто рассматривается как простая задача из-за отсутствия обновлений, устаревшей инфраструктуры в их среде и часто сетевой архитектуры в виде миски — ценность мониторинга нельзя недооценивать. с точки зрения защиты… Коммерческие субъекты обычно ищут самую быструю выплату, поэтому они быстро становятся заметными, как правило, потому, что пытаются монетизировать свой незаконный доступ. Обратное часто верно для национальных государств. Они больше заинтересованы в том, чтобы стать постоянным постоянным присутствием, поскольку это покупает им влияние и осведомленность. Если вы не можете отправить военно-морской флот в близлежащие международные воды ваших международных противников, вы можете попытаться проникнуть в их критически важную инфраструктуру, чтобы угрожать столь же болезненными последствиями».

Однако Джейсон Хикс (полевой директор по информационным технологиям и исполнительный советник Coalfire) отмечает, что пассивный мониторинг, вероятно, все еще является нормой просто из-за возраста и присущих используемому оборудованию ограничений: «Такие вещи, как обновления программного обеспечения, обычно поступают в эти среды через флешки. Кроме того, на многих устройствах работают специализированные операционные системы, которые не допускают сканирования на наличие уязвимостей и не поддерживают запуск вашего типичного пакета защиты конечных точек. Представьте, например, что ваш vuln scan отключит питание подстанции. Из-за всех этих факторов операторы редко имеют средства обеспечения видимости, ориентированные на безопасность, которые мы привыкли иметь в корпоративных сетях. Отрасль долгое время полагалась на автономную природу сетей OT для обеспечения безопасности. таким образом, инвестиции в мониторинг были бы направлены на повышение времени безотказной работы, а не на сбор телеметрии безопасности. Если вы хотите закрыть брешь в мониторинге, вам обычно остаются пассивные решения, разработанные для сред OT».

«Традиционно вам приходилось приобретать и управлять полностью отдельными LAN и WAN для ваших систем OT, поскольку из-за финансового давления некоторые фирмы пытаются найти способы использовать свою основную инфраструктуру для снижения затрат. Эти новые тенденции, вероятно, являются источником взломов OT, отмеченных в опросе, поскольку в прошлом для взлома сети OT требовался физический доступ. Я ожидаю увеличения инвестиций в защиту сред OT в ближайшем будущем», — отметил Хикс». ***(Scott Ikeda. ICS Cybersecurity Report: Control Systems Remain Highly Targeted by Threat Actors as Organizations Forced to Rapidly Mature Programs // CPO Magazine (https://www.cpomagazine.com/cyber-security/ics-cybersecurity-report-control-systems-remain-highly-targeted-by-threat-actors-as-organizations-forced-to-rapidly-mature-programs/). 10.11.2022).***

***

«Ежегодное исследование рабочей силы в области кибербезопасности (ISC)² показывает, что в настоящее время работает больше профессионалов в области кибербезопасности, чем в любой другой момент, но эта область все еще очень далека от полного укомплектования кадрами. Несмотря на рекордные 4,7 миллиона человек во всем мире, которые сейчас работают, по-прежнему существует нехватка рабочей силы в 3,4 миллиона человек, рост которой все еще недостаточно силен, чтобы решить эту проблему в течение следующих нескольких лет.

Карьера в области кибербезопасности вызывает растущий интерес, но по-прежнему существует огромный дефицит рабочей силы

Исследование Cybersecurity Workforce Study включало в себя участие более 11 700 активных сотрудников отрасли и найма лиц, принимающих решения, для организаций по всему миру.

По сравнению с прошлым годом штат специалистов по кибербезопасности вырос чуть более чем на 11 %, заполнив еще 464 000 вакансий. В большинстве регионов наблюдается рост найма на 12-15%, при этом Азиатско-Тихоокеанский регион лидирует с показателем 15,6%; Северная Америка отставала с ростом всего на 6,2%, а Австралия и Южная Корея сталкивались с аналогичными трудностями, чтобы не отставать. Некоторые отдельные страны резко выросли в росте, во главе с Нидерландами (64,3%) и Японией (40,4%). Только в Германии и Сингапуре количество незаполненных должностей увеличилось.

На первый взгляд это может показаться хорошей новостью для работодателей, но, к сожалению, спрос по-прежнему опережает этот рост, что приводит к увеличению дефицита международной рабочей силы немногим более чем в два раза по сравнению с темпами заполнения вакансий (26,2% в год). годовой прирост). Среди регионов Азиатско-Тихоокеанский регион снова был лидером, компенсировав скачок найма 52%-ным ростом спроса; Латинская Америка была единственным регионом, в котором наблюдалось снижение спроса (около 26%). Среди отдельных стран в Индии наблюдается колоссальное увеличение спроса на 630% всего за год, во Франции — на 120,6%, а во многих других — от 55% до 75%.

Отдельные отрасли испытывают особые проблемы с набором достаточного количества специалистов по кибербезопасности: правительственные учреждения, аэрокосмическая промышленность, образование, страхование и транспорт сообщают о самой большой нехватке. В целом по всем отраслям 70% респондентов говорят, что их организация недостаточно укомплектована персоналом, чтобы ее программа кибербезопасности была эффективной. Из тех, кто так считает, 50% заявили, что организация подвергается «умеренному» или «чрезвычайному» риску кибератаки из-за нехватки персонала.

Приоритеты также изменились среди тех, кто сообщает о проблемах безопасности из-за нехватки рабочей силы. В 2021 году основными проблемами, о которых они сообщали, были неправильно настроенные системы и нехватка времени для надлежащей оценки рисков и управления ими. Оценка рисков остается на первом месте в списке проблем, но другие проблемы, связанные с нехваткой кадров в области кибербезопасности, увеличили этот список: исправление критических

систем, нехватка времени для обучения всех членов группы кибербезопасности и упущения в процессах и процедурах.

Можно ли укрепить кадры кибербезопасности?

Судя по данным за этот и прошлый год, разумно ожидать, что глобальная нехватка рабочей силы не будет полностью устранена, по крайней мере, в течение следующих нескольких лет. Однако нехватка кадров такого масштаба в области кибербезопасности представляет серьезные риски даже на уровне национальной безопасности.

По большей части нехватка рабочей силы является простой проблемой спроса и предложения; резкое увеличение количества киберпреступлений, которое в настоящее время не показывает признаков замедления, создает спрос на квалифицированные кадры, которого просто не существует в необходимом количестве. Однако респонденты говорят, что более серьезной проблемой могут быть и другие проблемы: те, кто активно конкурирует за кадры в области кибербезопасности, говорят, что текучесть кадров является очень серьезной проблемой, что заработная плата неконкурентоспособна и что это часто связано с неадекватным бюджетом на кибербезопасность или ИТ. 22% также сказали, что они считают, что руководство неправильно распределяет ресурсы, перегружая ту или иную область слишком большим количеством своих квалифицированных специалистов.

Среди относительно небольшого числа организаций, которые не испытывают нехватки, что делается для того, чтобы сотрудники, занимающиеся кибербезопасностью, оставались заинтересованными в своих должностях и оставались довольны работой? Эта подгруппа респондентов говорит, что возможности внутреннего обучения, предлагающие работу на дому и ротацию рабочих мест, особенно эффективны и особенно успешны в крупных компаниях, где работает не менее 1000 человек.

Большинство организаций также рассматривают возможность автоматизации для решения проблемы нехватки рабочей силы. 57% уже внедрили какие-то меры автоматизации, а еще 26% говорят, что планируют внедрить их в будущем. Основное внимание в этих системах уделяется высвобождению существующей рабочей силы, чтобы тратить больше времени на решение задач более высокого уровня.

Нехватка кадров в области кибербезопасности также менее распространена в организациях, в которых менеджеры по найму ИТ имеют прочные рабочие отношения с отделом кадров, но только 52% респондентов в целом говорят, что именно так обстоят дела в их компании. 40% лиц, принимающих решения по найму, прямо заявили, что отдел кадров не добавляет ценности процессу.

Со своей стороны, квалифицированные сотрудники говорят, что недовольство на рабочем месте больше связано с проблемами корпоративной культуры, чем с тем, что их просят делать на работе. Большинство сказали, что они сменили работу за последние два года из-за лучшей оплаты и возможностей, но за этими факторами сразу же последовали негативная или нездоровая корпоративная культура, чувство выгорания и плохой баланс между работой и личной жизнью. Только около 50% говорят, что они, вероятно, сохранят свою нынешнюю позицию в течение следующих пяти лет». ***(Scott Ikeda. Study Shows Privacy Awareness Is the “New***

Normal" for Consumers, Online Behavior Is Much More Guarded // CPO Magazine (https://www.cpomagazine.com/cyber-security/cybersecurity-workforce-is-growing-but-worldwide-workforce-gap-of-3-4-million-continues-to-present-problems/). 03.11.2022).

***

«Кибербезопасность сейчас может быть самой напряженной работой в сфере технологий. Но может быть (крошечный) проблеск света в конце туннеля.

Согласно новому исследованию, почти треть директоров по информационной безопасности (CISO) и менеджеров по ИТ-безопасности в Великобритании и США рассматривают возможность ухода из своей нынешней организации.

Не только это, но и треть планируют бросить свою работу в течение следующих шести месяцев.

Фирма по кибербезопасности BlackFog опросила более 400 лиц, принимающих решения в области ИТ, в компаниях с более чем 500 сотрудниками в США и Великобритании, чтобы понять проблемы, с которыми они столкнулись в условиях растущих угроз ИТ-безопасности и нехватки квалифицированных специалистов в отрасли.

Выяснилось, что многие лидеры в области ИТ-безопасности изо всех сил пытаются не отставать от развивающихся угроз и новых методов кибербезопасности, а также сообщают о проблемах, связанных с наймом, удержанием и балансом между работой и личной жизнью, которые побуждают многих отворачиваться от отрасли.

Отвечая на вопрос о том аспекте своей роли, который им больше всего не нравится, 30% сослались на отсутствие баланса между работой и личной жизнью, а 27% заявили, что много времени тратится на «тушение пожаров», а не на решение стратегических вопросов бизнеса.

Помимо 32 % директоров по информационной безопасности, планирующих уход из -за стресса на работе, 52 % признались, что им трудно идти в ногу с новыми структурами и моделями, такими как Zero Trust, в то время как еще 20 % считают, что правильные навыки в их команде были «серьезной проблемой».

Из 32% респондентов, рассматривающих возможность ухода с должности, 33% заявили, что сделают это в течение следующих шести месяцев, а 37% заявили, что готовы покинуть корабль в течение следующих 7-12 месяцев.

Исследование BlackFog отражает растущую озабоченность лидеров кибербезопасности по поводу их способности обеспечивать безопасность бизнеса и потребителей в условиях роста киберпреступности и серьезной нехватки специалистов по кибербезопасности.

Это также подчеркивает огромную нагрузку, с которой сталкиваются специалисты по кибербезопасности, которые все чаще покидают профессию из-за стресса, выгорания и проблем с благополучием.

В отчете BlackFog было несколько крупиц хороших новостей. Например, лидеры в области кибербезопасности считают, что наконец-то достучались до лидеров компаний: 75% опрошенных BlackFog считают, что существует «полное соответствие» между ожиданиями совета директоров и тем, что способны обеспечить директора по информационной безопасности.

На самом деле, две трети (64%) респондентов заявили, что они могут выполнять свои приоритетные задачи в течение первых шести месяцев после начала работы. Компания BlackFog обнаружила, что в среднем 27% расходов на ИТ идет на финансирование безопасности, и директора по информационной безопасности, похоже, этим довольны.

Директора по информационной безопасности также сообщают о целеустремленности своих ролей: 44% респондентов опроса BlackFog заявили, что наиболее приятным аспектом их роли является выполнение роли «защитника» компании и чтобы люди работали в безопасных условиях. Даррен Уильямс, генеральный директор и основатель BlackFog, сказал, что, хотя роль лидеров кибербезопасности сопряжена с «огромными проблемами и огромным давлением», есть «обнадеживающие признаки» того, что боссы прислушиваются к их опасениям и соответствующим образом согласовывают свои бюджеты и бизнес-приоритеты.

Уильямс добавил: «Однако ключевым моментом является адаптация к быстро меняющейся среде, и организациям необходимо обеспечить, чтобы их команды безопасности получали время и ресурсы, чтобы идти в ногу с последними идеями, платформами и инновациями, разработанными для снижения их кибер-рисков». ***(Owen Hughes. Cybersecurity leaders want to quit. Here's what is pushing them to leave // ZDNET (https://www.zdnet.com/article/cybersecurity-leaders-want-to-quit-heres-what-is-pushing-them-to-leave/). 09.11.2022).***

***

«Кибербезопасность, кодирование и навыки работы с данными подобны золотой пыли — и спрос в 2023 году будет только расти.

Спрос на цифровые навыки значительно вырос в 2022 году. По мере того, как все больше компаний используют технологии для инноваций и обеспечения будущего своего бизнеса, количество доступных талантов в области программного обеспечения, способных достичь этих целей, продолжает сокращаться.

Хотя это создало серьезные проблемы с наймом для компаний, квалифицированные специалисты в области технологий оказались в очень выгодном положении, когда речь идет о возможностях трудоустройства и переговорах.

Заглядывая в будущее до 2023 года, картина остается почти такой же. В то время как риск рецессии заставит больше компаний замедлить или приостановить найм в попытке сократить расходы или «оптимизировать», влияние на найм технологий будет сравнительно небольшим. Действительно, даже во время экономического спада технологии остаются (по крайней мере, на данный момент) довольно безопасным местом.

Одним из секторов, нуждающихся в талантах, является кибербезопасность. Согласно отчету Secureworks Boardroom Cybersecurity Report за 2022 год, количество открытых вакансий в области кибербезопасности во всем мире выросло на 350% в период с 2013 по 2021 год, с 1 миллиона до 3,5 миллионов.

Саймон Хепберн, генеральный директор Совета по кибербезопасности Великобритании, говорит, что потребность в навыках кибербезопасности в Великобритании особенно велика: по оценкам, 14 100 вакансий в настоящее время остаются незаполненными.

По словам Хепберн, даже несмотря на то, что угроза рецессии ложится тяжким бременем на умы руководителей компаний, работодатели не могут экономить на квалифицированных специалистах по ИТ-безопасности в 2023 году. операционная дисфункция, потеря доходов и значительный ущерб репутации», — говорит Хепберн ZDNET.

«Это не те риски, на которые организации захотят пойти, когда они уже решают двойные проблемы безудержной инфляции и надвигающейся рецессии».

Стало совершенно ясно, что одни только технологии не могут решить проблему.

Дэвид Махди, CSO и советник по информационной безопасности в поставщике цифровой идентификации Sectigo, говорит, что компаниям нужны лидеры в области безопасности, которые могут внедрить осведомленность о кибербезопасности в коллективное мышление организации. «Вы можете окружить своих сотрудников новейшими брандмауэрами и антивирусным программным обеспечением, но только тогда, когда вы научите их, как обеспечить безопасность своей онлайн-идентификации на рабочем месте, вы сможете создать надежную систему кибербезопасности», — говорит Махди ZDNET.

Прошли те времена, когда сотрудники могли просто использовать девичью фамилию своей матери в качестве пароля с несколькими цифрами и специальными символами в конце. «Лучшая технология безопасности просто не поможет, если вы не будете постоянно учиться», — добавляет Махди.

«Умение защитить себя на индивидуальном уровне становится все более важным навыком».

Обращение ко всем кодерам

Кодирование также будет пользоваться постоянным и интенсивным спросом в 2023 году и далее.

Согласно недавнему отчету Randstad, в период с 2018 по 2021 год количество объявлений о вакансиях для инженеров по обработке данных выросло на 116%, а количество объявлений для специалистов по информатике увеличилось на 72%. Руководство Роберта Халфа по зарплате на 2023 год также выявило устойчивый спрос на разработчиков, особенно на тех, кто знает C#, C++, Angular, Node.js, AWS, Google Cloud Platform и Azure.

Кристиан Минеа (Christian Minea), руководитель отдела кадров в hackajob, говорит, что C# и Java оказались одними из самых востребованных навыков на платформе hackajob.

Согласно данным, опубликованным hackajob в сентябре 2022 года, Java-программисты обеспечили наибольшую долю трудоустройства, на их долю пришлось 15,8% рыночных наймов в 2021-2022 годах. За ними следуют разработчики C# (15,3%), специалисты DevOps (10,8%), программисты JavaScript (10,6%) и специалисты по обеспечению качества, на долю которых приходится 8,9% отраслевых размещений.

«Глядя на нашу статистику за последние два года, самые популярные технические роли, на которые мы назначаем кандидатов, — это Java и C#, и мы ожидаем, что эта тенденция сохранится в 2023 году», — сказал Минеа ZDNET.

«Интересно, что мы видим, что многие бэкенд-разработчики указывают Golang в своих резюме — не как коммерческий навык, а как то, чему они учатся в свободное время. Мы ожидаем, что это будет иметь эффект снежного кома и превратит его из простого интереса в до обязательного навыка, и, скорее всего, в ближайшие несколько лет его популярность будет расти».

Должности разработчиков также продолжают оставаться одними из самых высокооплачиваемых: согласно статистике недавнего исследования Marketplace Monitor, проведенного hackajob, в котором анализируются технические таланты и тенденции найма за последние 12 месяцев, установлено, что начальная заработная плата инженеров-программистов на 64% выше, чем в среднем по Великобритании.

«Для более опытных технических работников шестизначная зарплата является обычным явлением, плюс бонусы и акции. Это также означает, что кандидаты часто могут уверенно отказаться от возможности трудоустройства, если зарплата не соответствует ожиданиям», — добавляет Минеа.

В сочетании с навыками, связанными с облачными технологиями, разработчики могут защитить себя от рецессии, освоив современные процессы доставки программного обеспечения, в частности DevOps.

«Поскольку DevOps занимает центральное место в том, как организации ускоряют свой путь к получению ценности с помощью программного обеспечения, развитие навыков управления и истинное понимание рабочих операций гарантируют, что разработчики опередят конкурентов», — говорит Джон Смит, технический директор Veracode.

«Освоив современные процессы доставки программного обеспечения, разработчики смогут продемонстрировать, как они могут повысить ценность и напрямую решать бизнес-задачи».

Новый тип разработчика программного обеспечения?

По мере ускорения масштабов и роста разработки программного обеспечения, а также с постоянными разработками ИИ в программировании и инженерии требования к роли разработчиков программного обеспечения также, похоже, будут меняться.

«AI/ML меняет мир программирования так же, как калькулятор и компьютер изменили мир», — говорит Сторми Питерс, вице-президент GitHub по сообществам. «Эти технологические достижения берут на себя большую часть рутинной, рутинной работы, которой разработчики когда-то должны были посвящать все свое время. Теперь разработка выглядит иначе».

Эти достижения, по словам Питерса, высвободили время для более пристального внимания к решению важных проблем и более широкой картине. По мере того, как мы вступаем в 2023 год, а разработка программного обеспечения остается в центре бизнес-стратегий, решение проблем, критическое мышление и другие человеческие навыки окажутся неотъемлемыми. «Несмотря на то, что новые технологии все чаще позволяют им оставаться в потоке и решать сложные проблемы, технические аспекты, связанные с программированием, проектированием и разработкой кода благодаря высокому уровню понимания ИИ, DevOps и языков программирования, также будут оставаться центральными по важности. к дисциплине», — добавляет она.

Действительно, Сандер ван'т Норденде, генеральный директор Randstad, говорит, что быстрый рост ИИ и других технических инноваций изменит не только то, как люди работают, но и «навыки, необходимые для процветания в цифровой экономике», включая те навыки, которые только врожденные. людям.

«Спрос на людей, обладающих знаниями в области машинного обучения, науки о данных, визуализации данных и навыков работы с социальными сетями, распространяется по секторам быстрее, чем спрос на средние навыки», — говорит Норденде ZDNET.

«Человеческие качества, которые отличают нас от машин, такие как эмпатия и креативность, по-прежнему имеют решающее значение на рынках труда и талантов, и работодатели должны отдавать им приоритет наряду с техническими навыками».

Вызов для лидерства

Лидерство также будет иметь ключевое значение для поддержания стабильности роста в течение следующих 12 месяцев, особенно проблемы с наймом, удержанием и повышением квалификации продолжают влиять на бизнес.

Мелина Маснатта, глобальный директор по обучению и DEI в Globant, считает, что инвестирование времени и ресурсов в управленческие навыки и диверсификацию лидерства является «одним из самых важных действий, которые должны предпринять сейчас как компании, так и отдельные лица».

В частности, Маснатта говорит, что лидеры будут нести ответственность за предоставление структуры и ресурсов для развития навыков среди команд и эффективное управление повышением квалификации в рамках всей организации. «Лидер будет обязан привлекать и расширять возможности своих команд, часто удаленно», — сказал Маснатта ZDNET.

«Высокоэффективная рабочая среда обусловлена высокой психологической безопасностью в командах. Будущие и нынешние лидеры сталкиваются с проблемой укрепления этой психологической безопасности на расстоянии». ***(Owen Hughes. Cybersecurity, cloud and coding: Why these three skills will lead demand in 2023 // ZDNET (https://www.zdnet.com/article/cybersecurity-cloud-and-coding-why-these-three-skills-will-lead-demand-in-2023/). 09.11.2022).***

***

«Сегодняшние проблемы с безопасностью еще предстоит решить. Но развитие технологий и быстро меняющийся мир также означают появление новых проблем.

Год — это большой срок для кибербезопасности.

Конечно, есть некоторые константы. Программа-вымогатель уже много лет является серьезной проблемой кибербезопасности, но не собирается исчезать по мере того, как киберпреступники продолжают развивать свои атаки. И значительное количество корпоративных сетей остаются уязвимыми, часто из-за недостатков безопасности, для которых уже давно доступны обновления.

Но даже если вы считаете, что знаете обо всех уязвимостях программного обеспечения в вашей сети, постоянно появляются новые недостатки безопасности, и некоторые из них могут иметь серьезные последствия.

Возьмите недостаток Log4j: год назад он был совершенно неизвестен, скрываясь в коде. Но после того, как об этом стало известно в декабре, глава CISA назвал это одним из самых серьезных недостатков. В конце 2022 года это по-прежнему часто является прямой уязвимостью в системе безопасности, скрытой в коде многих организаций, и это, вероятно, сохранится в далеком будущем.

Нехватка навыков безопасности

Какие бы последние хакерские уловки или дыры в безопасности ни обнаружили исследователи, люди, а не технологии, всегда лежат в основе кибербезопасности, и к добру, и к злу.

Этот фокус начинается с того, что на базовом уровне сотрудники могут идентифицировать фишинговую ссылку или мошенничество с компрометацией деловой электронной почты, а начальство нанимает правильную группу информационной безопасности, которая помогает устанавливать и контролировать корпоративную защиту.

Но навыки кибербезопасности пользуются большим спросом, поскольку персонала просто не хватает.

«Поскольку киберугрозы становятся все более изощренными, нам нужны ресурсы и необходимые навыки для борьбы с ними. Потому что без специализированных талантов организации действительно подвергаются риску», — говорит Келли Розумальский, старший вице-президент и руководитель национальной киберзащиты в Booz Allen. Гамильтон.

«Нам нужно поощрять людей из самых разных областей — от компьютерной инженерии и программирования до психологии — изучать кибербезопасность, потому что для того, чтобы мы действительно выиграли войну с талантами, мы должны быть привержены не только найму, но и созданию, удержанию и инвестированию. в нашем таланте», — говорит она.

Очень важно, чтобы в организациях были люди и процессы для предотвращения или обнаружения кибератак. Существует не только постоянный повседневный риск фишинга, вредоносных атак или кампаний вымогателей со стороны банд киберпреступников, но и угроза со стороны хакеров и враждебных государств.

Новые и более серьезные угрозы цепочке поставок

Хотя киберпространство уже некоторое время является ареной международного шпионажа и других кампаний, текущая глобальная геополитическая обстановка создает дополнительные угрозы.

«Мы возвращаемся к геополитической парадигме, предполагающей конкуренцию великих держав, — место, где мы не были уже несколько десятилетий», — говорит Мэтт Горхэм, руководитель института инноваций в области кибербезопасности и конфиденциальности в PwC и бывший помощник директора отдела кибербезопасности ФБР. Разделение.

«И мы делаем это, когда в киберпространстве нет настоящего консенсуса, красных линий или норм», — добавляет он.

Например, технология, задействованная в управлении критической инфраструктурой, стала мишенью для России во время ее продолжающегося вторжения в Украину.

За несколько часов до начала вторжения у провайдера спутниковой связи Viasat произошел сбой, в результате которого была нарушена широкополосная связь в Украине и других странах Европы — инцидент, который западные спецслужбы приписывают России. Илон Маск также заявил, что Россия пыталась взломать системы Starlink, сети спутниковой связи, управляемой его ракетной фирмой SpaceX, которая обеспечивает доступ в Интернет для Украины.

Но это происходит не только в зоне боевых действий, где враждебные государства пытаются вызвать сбои с помощью кибератак: организации, особенно те, которые участвуют в критически важных цепочках поставок, также становятся мишенью поддерживаемых государством хакеров.

Только посмотрите, как российские хакеры скомпрометировали крупного поставщика программного обеспечения с помощью вредоносного ПО, которое вытолкнуло вредоносное обновление, предоставив лазейку в сети нескольких правительственных учреждений США.

«Опасения всегда вызваны реальными событиями. Поэтому за последние пару лет мы стали свидетелями атак на цепочки поставок со стороны государства, которые заставили всех задуматься о связанном с этим риске цепочки поставок», — говорит Горхэм, который призывает организации подумать не только о том, как они могут предотвратить кибератаки, но и о том, как обнаруживать злонамеренные вторжения в сеть и надлежащим образом реагировать на них.

«Если государство намерено проникнуть в ваши системы, у них есть для этого ресурсы и возможности, поэтому речь идет об их обнаружении и изгнании», — добавляет он.

Зачастую взломщикам позволяют проникнуть в сеть не сложные методы, а распространенные уязвимости, такие как слабые пароли, неприменение обновлений безопасности или отсутствие двухфакторной аутентификации (2FA). А иногда, особенно в случае критической инфраструктуры и промышленных сетей, программному обеспечению, на котором работают эти системы, может быть много лет.

Web3 и IoT: новые проблемы или возвращение к истокам?

Но только потому, что что-то новое, это также не означает, что оно автоматически безопасно — и, поскольку такие технологии, как Web3 и Интернет вещей (IoT), продолжают развиваться в 2023 году, они станут еще большей целью для кибератак и хакеров.

По-прежнему много ажиотажа вокруг потенциала Web3 — видения сети, которая отбирает контроль у крупных компаний и децентрализует власть среди пользователей с помощью блокчейна, криптовалюты и экономики, основанной на токенах.

Но, как и о любой новой технологии, особенно о той, которая вызывает много ажиотажа и ажиотажа, о безопасности часто забывают, поскольку разработка программного обеспечения спешит с выпуском продуктов и услуг, о чем свидетельствуют различные взломы криптовалютных бирж, где злоумышленники украли миллионы в криптовалюте.

«Люди в восторге от новых технологий. Затем они забывают учитывать недостатки безопасности, потому что так торопятся внедрить их. С Web3 мы

наблюдаем такую ситуацию, когда люди были возбуждены, чтобы начать — но безопасность остается позади», — говорит Кэти Пакстон-Фир, преподаватель кибербезопасности в Манчестерском столичном университете и охотник за ошибками в HackerOne.

Из-за этой ситуации охотники за ошибками находят множество уязвимостей в приложениях и службах Web3. Часто это серьезные уязвимости, которые могут быть чрезвычайно прибыльными для злоумышленников, если они обнаружат их первыми, и потенциально дорогостоящими для пользователей.

Но хотя некоторые из этих уязвимостей являются новыми и сложными, многие из нарушений безопасности, которые затронули криптовалютные биржи и другие службы Web3, были сведены к неправильно настроенным службам или фишинговым атакам, когда преступники завладели паролями.

Таким образом, хотя экспериментальные и необычные уязвимости представляют собой проблему, внедрение основ кибербезопасности может помочь остановить взломы Web3, особенно по мере того, как технология становится все более популярной и становится все более привлекательной мишенью для киберпреступников.

«Это похоже на то, что мы смотрим на эти действительно крутые новые уязвимости и восхищаемся ими, но забываем о таких вещах, как контроль доступа», — говорит Пакстон-Фир.

В то время как блокчейн и Web3 пока еще могут считаться нишевыми технологиями, Интернет вещей таковым не является: по всему миру установлены миллиарды устройств в домах и на рабочих местах, в том числе те, которые помогают поддерживать критически важную инфраструктуру и здравоохранение.

Но, как и в случае с другими новыми технологиями, существует риск того, что, если эти подключенные устройства не будут должным образом защищены, они могут быть нарушены или даже сделать уязвимыми целые сети. Это пробел, который необходимо учитывать, поскольку подключенные устройства становятся все более распространенными в нашей жизни.

«Мы находимся в очень сложном положении. Но мы должны обратить на это внимание», — говорит Розумальский из Booz Allen Hamilton. «Прямо сейчас злоумышленники могут проникнуть через медицинское устройство и использовать его в качестве опорной точки для уничтожения всей больничной сети — это, очевидно, может повлиять на уход за пациентами».

Она утверждает, что ключевым моментом является то, что больницам, поставщикам критической инфраструктуры любых других организаций необходимо признать, что кибербезопасность играет ключевую роль в процессах планирования и принятия решений в 2023 году, чтобы помочь обеспечить максимальную защиту сетей от угроз.

Перспективы кибербезопасности на 2023 год

«Безопасность должна быть за столом переговоров, и это очень, очень важно. Но вам нужно стратегически продумать, как снизить эти риски, потому что эти устройства важны», — говорит Розумальски, и она считает, что прогресс есть. с советами директоров, которые больше осведомлены о проблемах кибербезопасности. Однако предстоит еще много работы.

«Я думаю, что за последний год мы предприняли много шагов, которые начнут выставлять нас во все лучшем и лучшем свете и смогут по-настоящему бороться с некоторыми из этих угроз в будущем».

И она не единственная, кто считает, что, хотя кибербезопасность и бюджеты кибербезопасности по-прежнему требуют большего внимания, в целом все движется в правильном направлении.

«Все больше людей осознают, что это серьезная и масштабная угроза, а также существует значительный риск, — это вселяет в меня некоторый оптимизм», — говорит Горхэм из PwC, хотя он понимает, что кибербезопасность не станет внезапно идеальной. По мере того, как мир приближается к 2023 году, все еще будет много проблем, с которыми нужно справиться.

«Угроза не исчезает — она значительна и будет становиться еще более значительной по мере того, как мы продолжаем цифровую трансформацию. Но я думаю, что тот факт, что мы смирились с ней сегодня, — это хороший знак для будущего», — говорит он». ***(Danny Palmer. Cybersecurity: These are the new things to worry about in 2023 // ZDNET (https://www.zdnet.com/article/cybersecurity-these-are-the-new-things-to-worry-about-in-2023/#link={%22linkText%22:%22Cybersecurity:%20These%20are%20the%20new%20things%20to%20worry%20about%20in%202023%22,%22target%22:%22_blank%22,%22href%22:%22https:/www.zdnet.com/article/cybersecurity-these-are-the-new-things-to-worry-about-in-2023/%22,%22role%22:%22standard%22,%22absolute%22:%22%22}). 09.11.2022).***

***

«Мы ознакомились с прогнозами аналитиков. Это технологии и проблемы, которые будут иметь для вас значение в 2023 году.

По мере приближения конца года вступает в действие ежегодный ритуал определения технологических тенденций и прогнозирования следующей солнечной орбиты. Такие упражнения всегда интересны, но также и рискованны по своей сути, особенно в неопределенные времена, такие как те, которые мы недавно пережили и продолжаем переживать.

Например, в конце 2019 года мало кто мог предположить, что в следующем году мир труда перевернется с ног на голову из-за глобальной пандемии, что приведет к беспрецедентному вниманию к устройствам и услугам, облегчающим удаленную работу, и, вероятно, постоянный переход на гибридную модель.

Затем, когда экономика приспосабливалась к пандемии и восстанавливалась после нее, вторжение России в Украину в феврале 2022 года вызвало резкий рост цен на энергоносители, рост инфляции, проблемы с цепочками поставок и опасения по поводу широкомасштабной рецессии. Эта серия потрясений имеет серьезные последствия для ИТ-индустрии, которые, по всей видимости, продолжатся до 2023 года и далее.

Так что, возможно, самая большая польза от ежегодного раунда технических предсказаний заключается не столько в мелких деталях, которые часто теряются из-за контакта с неожиданными событиями, сколько в возможности оценить общее направление движения.

Давайте посмотрим на последние тенденции и прогнозы.

Что говорят аналитики

Гартнер

10 главных стратегических технологических тенденций Gartner на 2023 год сгруппированы по трем темам:

Оптимизация ИТ-систем для повышения надежности, улучшения процесса принятия решений на основе данных и поддержания целостности производственных систем искусственного интеллекта.

Масштабирование вертикальных предложений, увеличение скорости доставки продуктов и обеспечение возможности подключения повсюду.

Новаторское изменение бизнес-модели, новое взаимодействие с сотрудниками и клиентами и ускорение стратегий выхода на новые виртуальные рынки.

Основой всех этих тенденций является устойчивость: «Каждые инвестиции в технологии должны быть сопоставлены с их воздействием на окружающую среду, помня о будущих поколениях. «Устойчивость по умолчанию» как цель требует устойчивых технологий», — говорит Дэвид Грумбридж из Gartner. Подтверждением этой точки зрения является исследование Gartner CEO and Senior Business Executive Survey 2022 года, которое показало, что экологическая устойчивость была третьим по значимости фактором после производительности и качества среди 80% руководителей, планирующих инвестировать в новые продукты в 2022–2023 годах.

Вот 10 главных трендов Gartner:

Изображение: Гартнер

Цифровая иммунная система (DIS) использует различные методы, в том числе тестирование с использованием искусственного интеллекта и безопасность цепочки поставок программного обеспечения, для повышения качества и устойчивости критически важных для бизнеса систем. Прикладная наблюдаемость берет необработанные данные, добавляет контекст и аналитику, а также генерирует решения для бизнеса и ИТ на основе данных. Управление доверием, рисками и безопасностью ИИ (AI TRiSM) охватывает управление моделью ИИ, надежность, справедливость, надежность, устойчивость, эффективность и конфиденциальность.

Отраслевые облачные платформы сочетают в себе программное обеспечение, платформу и инфраструктуру как услугу с адаптированными отраслевыми

функциями. Инжиниринг платформ предоставляет инструменты, возможности и процессы, необходимые для оптимизации работы разработчиков и ускорения цифровой доставки. Реализация ценности беспроводной связи включает в себя предоставление ценности для бизнеса с помощью вычислений для конечных пользователей, периферийных устройств и цифровых меток (RFID).

Суперприложения — это сочетание приложения, платформы и экосистемы, где третьи стороны могут разрабатывать и публиковать свои собственные мини-приложения. Адаптивные системы искусственного интеллекта используют обратную связь в режиме реального времени, чтобы корректировать свое обучение и адаптироваться к меняющимся обстоятельствам в реальном мире. Metaverse — это «коллективное виртуальное трехмерное общее пространство» с экономикой, основанной на криптовалютах и NFT.

IDC

Прогнозы IDC для мировой ИТ-индустрии на 2023 год охватывают ключевые факторы на следующие пять лет, которые, как мы уже отмечали выше, скорее всего, столкнутся со значительными экономическими потрясениями. Или, как выразился аналитик Рик Вилларс: «В течение следующих нескольких лет ведущие поставщики технологий должны играть ведущую роль, помогая предприятиям использовать инновационные технологии, чтобы преодолевать нынешние бури перемен».

Вилларс отмечает, что надвигающаяся рецессия первым ударит по экономике «как услуга», в которой старая тактика, такая как отсрочка капитальных вложений (например, обновление оборудования и программного обеспечения), будет недоступна для ИТ-руководителей. Вместо этого, по словам Вилларса, в 2023 году акцент будет смещен на снижение операционных расходов (оптимизация расходов на облачные технологии, пересмотр контрактов XaaS, устранение дубликатов инструментов SaaS и концентрация на проектах, обеспечивающих наибольшую ценность для бизнеса), при этом необходимо более постоянное сокращение операционных расходов. 2024 г. и далее (за счет более низкой стоимости ИТ-единицы и снижения трудозатрат на администрирование).

Однако общий посыл более оптимистичен: «Технологии и ИТ — это не то, где мы сокращаем расходы, — технологии — это то, во что мы инвестируем, чтобы помочь остальному бизнесу справиться с рецессией», — говорит Вилларс. «Это продолжающийся переход к цифровому бизнесу, который мы начали наблюдать два года назад».

Для IDC «цифровой бизнес» охватывает все, от процессов, продуктов и услуг до опыта, и будет осуществляться «командой мечты», состоящей из ИТ и бизнес-подразделений.

Вот некоторые из ключевых прогнозов IDC:

В 2025 году для 60% предложений по инфраструктуре, безопасности, данным и сети потребуются облачные платформы управления, которые обеспечивают обширную автоматизацию и обещают значительное сокращение текущих эксплуатационных расходов.

К 2024 году недостатки в создании критически важных навыков и усилиях по обучению лидеров ИТ-индустрии не позволят 65% предприятий получить полную отдачу от инвестиций в облака, данные и автоматизацию.

Суверенные заявления об устойчивости, отказоустойчивости и местонахождении активов до 2025 года заставят ИТ-директоров перераспределять персонал, бюджеты и операционные процессы для более чем 35% ИТ-активов и активов данных.

В 2023 году 70 % предприятий, внедряющих инфраструктуру/программное обеспечение как услугу, будут больше сдерживаться неспособностью оценить обещания более быстрых инноваций и операционных выгод, чем проблемами затрат.

К концу 2024 года 60 % предложений платинового уровня как услуг в области безопасности, бизнес-операций и DaaS будут включать в себя пакетный доступ к специализированным группам малого и среднего бизнеса, чтобы помочь уменьшить влияние нехватки навыков.

В 2026 году 45% предприятий G2000 будут по-прежнему сталкиваться с существенными рисками из-за нежелания передовых работников и руководителей бизнеса доверять действиям, инициированным проверенными автономными техническими системами…

Изображение: IDC

Последняя мысль IDC на 2024 год и далее заключается в том, что автоматизация ИТ-операций, бизнес-процессов и разработки приложений будет иметь решающее значение для масштабирования цифрового бизнеса.

«Мы создаем совершенно новую систему доставки технологий — более надежную, более безопасную, более устойчивую, и это будет задача, которую предстоит решать ИТ-директорам», — говорит Вилларс.

Форрестер

По словам Forrester, в трудные времена организациям необходимо сконцентрироваться на своих основных задачах и сильных сторонах: «В 2023 году умные бизнес-лидеры сосредоточатся на усилиях, которые не приносят плодов, и отдадут приоритет долгосрочному росту. Экономические и геополитические потрясения посеют страх и разрушение, но паника, недальновидный захват доходов и плохо спланированное возвращение в офис только усугубят ситуацию».

Вот некоторые из ключевых прогнозов Форрестера:

Потребители осторожны, но не сокращают расходы.

Нехватка навыков ставит под угрозу способность CX-команд процветать.

Мониторинг технологий раздражает сотрудников.

Гринвошинг становится серьезным бизнес-риском.

Руководители пытаются заставить сотрудников вернуться в офис, что приводит к плачевным результатам.

Эксперименты с метавселенной не способны захватить воображение публики.

Нехватка талантов заставляет технических руководителей искать новые источники кандидатов.

Скандалы в технологических компаниях подрывают доверие потребителей.

По словам Forrester, ключевым приоритетом бизнеса и технологий на 2023 год является доверие — в разных формах. «Клиенты все больше устают от того, что организации играют быстро и свободно с их личными данными, и регулирующие органы не сильно отстают. И это не остановится на достигнутом — подпитываемые гневом сытых по горло клиентов и сотрудников, регулирующие органы будут тщательно изучать гринвошинг, дезинформацию и наблюдение за сотрудниками».

CCS Insight

Одной исследовательской фирмой, занимающейся подробным прогнозированием, является CCS Insight, которая недавно провела трехдневное онлайн-мероприятие, на котором были представлены презентации аналитиков, интервью с руководителями Samsung, EE и Qualcomm и не менее 100 прогнозов.

Прогнозы CCS Insight на 2023 год сгруппированы по 10 категориям: кремниевые основы, устойчивое развитие, развитие инфраструктуры, провайдеры подключения, регулирование, новые возможности, личное будущее, изменение рабочего места, виртуальные миры и подключенные устройства.

Вместо того, чтобы перечислять все 100 прогнозов, я выбрал пару из каждой категории, которые привлекли мое внимание:

Категория	**Прогноз**
Силиконовые основы	Попытки сбалансировать географическое разнообразие производства полупроводников терпят неудачу, и Тайвань сохраняет свое лидерство
	К 2025 году квантовые компьютеры достигнут 60-секундного времени когерентности
устойчивость	К 2027 году мобильные приложения позволят пользователям отслеживать свой углеродный след в режиме реального времени.
	К 2024 году разрабатывается международный стандарт для расчета выбросов углекислого газа облачных сервисов.
Развитие инфраструктуры	Раннее развитие 6G в Китае привело к появлению как минимум двух конкурирующих стандартов на Востоке и Западе.
	К 2024 году крупная мобильная сеть выйдет из строя из-за одновременного отказа нескольких DNS-шлюзов.

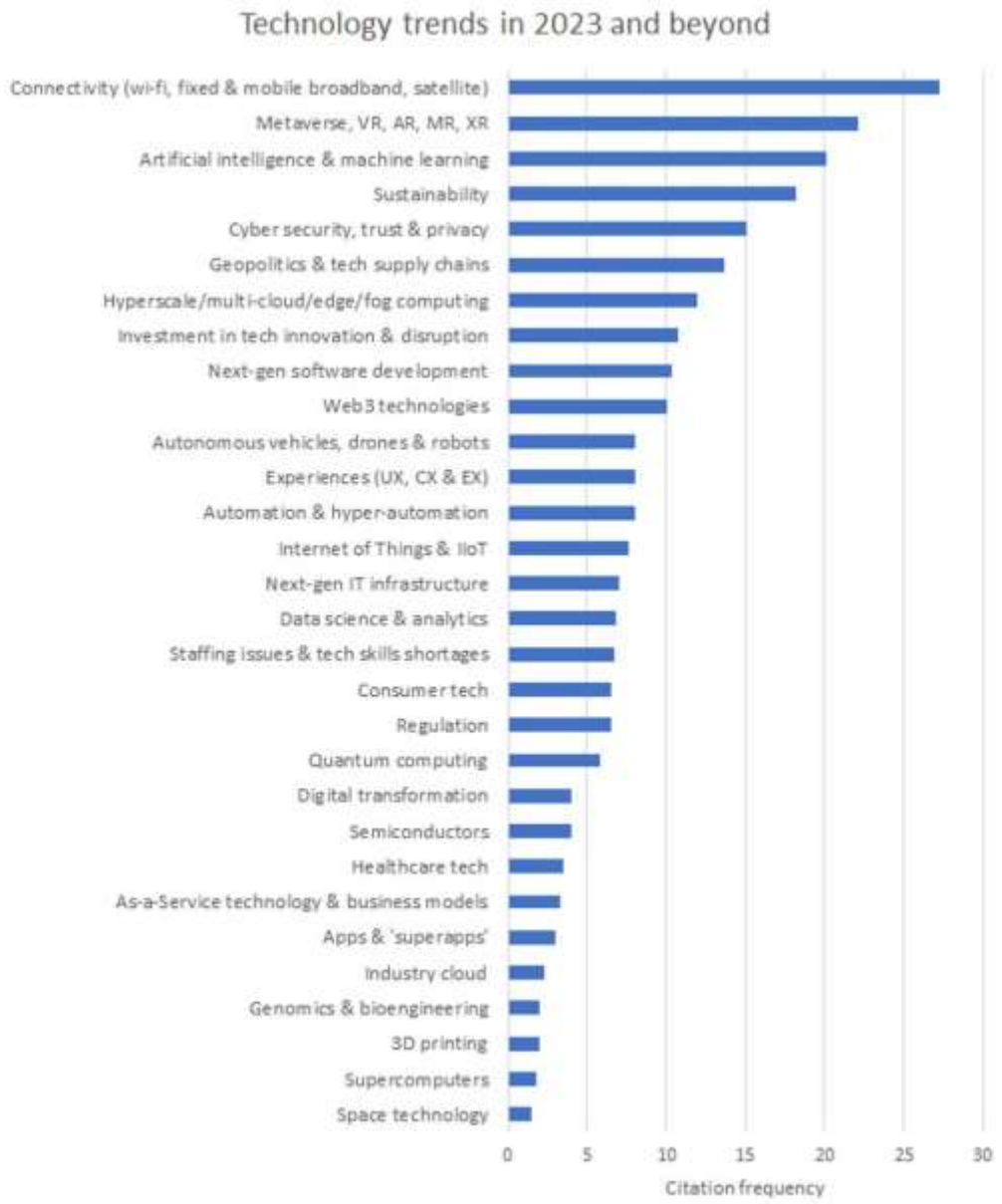
Поставщики подключения	К 2025 году провайдер спутникового широкополосного доступа Starlink будет выделен из SpaceX как публичная компания.
	К 2025 году не менее 25 операторов связи будут предлагать услуги подключенных автомобилей в качестве дополнения к потребительским планам 5G.
Регулирование	Закон ЕС о цифровых рынках отменяет предпочтительное размещение продуктов в результатах поиска к 2024 году.
	Явные признаки российско-китайского «сплинтернета» появятся к 2023 г.
Новые возможности	Apple войдет в бизнес медицинского страхования США в 2024 году
	К 2026 году больше компаний будут следовать за Теслой в инвестировании в цепочки поставок полезных ископаемых.
Личные фьючерсы	К 2028 году «ваш блокчейн» позволит разработчикам создавать жизнеспособных цифровых двойников людей для поддержки персонализированных услуг.
	К 2030 году интеллектуальный беспроводной мониторинг тела приведет к всеобъемлющему и персонализированному медицинскому обслуживанию.
Смена рабочего места	К 2024 году корпоративные инструменты для совместной работы добавят иммерсивные пространства, чтобы помочь воспроизвести работу в офисе.
	Спрос на программное обеспечение, которое измеряет и отслеживает связь между опытом сотрудников и клиентами, в 2023 году резко возрастет.
Виртуальные миры	Компания Apple в области пространственных вычислений полностью избегает использования устоявшейся терминологии, такой как виртуальная реальность, дополненная реальность или метавселенная.
	К 2025 году Meta выпускает гарнитуру виртуальной реальности, управляемую встроенным нейронным датчиком.

Подключенные устройства	К концу 2026 года более 25 миллионов человек выходят в Интернет через мобильный телефон, подключенный напрямую к спутникам. Apple выпустит складной iPad в 2024 году

В ходе панельной дискуссии на мероприятии аналитики CCS Insight обсудили, как спутниковая связь может дополнить, а не узурпировать наземные фиксированные и мобильные сети, отметив при этом недавний шквал объявлений о спутниковых услугах от производителей смартфонов. Участники дискуссии также обсудили состояние дел в метавселенной, устойчивых технологиях и умном доме.

Обзор прогнозов на 2023 год

Очевидно, что в прогнозах аналитиков, описанных выше, есть что переварить. Чтобы попытаться получить общую картину, мы взяли эти и прогнозы из ряда других недавних прогнозных исследований и статей и распределили их по возникающим категориям. Вот как выглядит получившаяся диаграмма:



Данные и диаграмма: ZDNET

Неудивительно, что возможности подключения — Wi-Fi, фиксированная и мобильная широкополосная связь, а также спутниковая связь — возглавляют рейтинги, поскольку именно они лежат в основе всего цифрового мира. Аналогичным образом, заметные результаты в области искусственного интеллекта (ИИ) и машинного обучения (МО), кибербезопасности, облачных вычислений и разработки программного обеспечения не являются неожиданными. Второе место метавселенной, наряду с VR/AR/MR/XR, подтверждает ее статус самой разрекламированной технологии на данный момент, а присутствие «Геополитики и технологических цепочек поставок» на шестом месте является признаком времени.

Мынадеемся, что более постоянным вожаком является обладатель четвертого места: устойчивость. Поскольку важность борьбы с изменением климата признают все, кроме тех, кто имеет корыстные или идеологические интересы, приятно видеть, что так много аналитиков и экспертов включают экологические соображения в свои прогнозы об устройствах, компонентах ИТ-инфраструктуры и сетях, которые их соединяют». ***(Charles McLellan. Tech in 2023: Here's what is going to really matter // ZDNET (https://www.zdnet.com/article/tech-in-2023-weve-analysed-the-data-and-heres-whats-really-going-to-matter/#link={%22linkText%22:%22Tech%20in%202023:%20We've%20analysed%20the%20data,%20and%20here's%20what's%20really%20going%20to%20matter%22,%22target%22:%22_blank%22,%22href%22:%22https:/www.zdnet.com/article/tech-in-2023-weve-analysed-the-data-and-heres-whats-really-going-to-matter/%22,%22role%22:%22standard%22,%22absolute%22:%22%22}). 14.11.2022).***

***

«В следующем году произойдут большие скачки вперед для одних технологий и крошечные, но важные шаги для других.

Все думают о технологиях как о быстро развивающейся отрасли, и во многом это правда.

Наверняка есть область технологической индустрии, полностью населенная типами «двигай быстро и ломай вещи», которые спешат создать минимально жизнеспособный продукт и говорят о таких вещах, как «NFT» и «Web 3».

Но есть и другие регионы, где медленное наращивание слоев технологии означает, что, хотя старые инструменты могут быть вытеснены более новыми инновациями, они не всегда забываются (например, те факсимильные аппараты).

Все это, наряду с риском, присущим любым попыткам прогнозирования в наши дни, означает, что разработка набора технологических тенденций на предстоящий год может быть сложной задачей. Но мы поговорили с аналитиками, проанализировали данные и использовали опыт всей команды ZDNET при создании специального отчета за этот месяц, целью которого является дать вам хотя бы приблизительное представление о том, как будут выглядеть технологии в 2023 году.

И есть несколько более крупных тенденций, в которых мы можем быть достаточно уверены.

Разработчики, облака и многое другое

Спрос на технических работников не исчезает, даже несмотря на то, что на данный момент крупные технологические компании отказались от найма. Это потому, что последние пару лет продемонстрировали преимущества расходов на технологии. Будь то предоставление новых способов связи с клиентами (и продажи им) или поддержка персонала, работающего в гибридном режиме, расходы на технологии теперь рассматриваются руководителями как инвестиции, которые приносят реальную пользу.

Для многих организаций преодоление трудностей последних нескольких лет означало быстрое ускорение использования и признания технологий. Вот почему многие аналитики ожидают роста расходов, даже если 2023 год будет тяжелым для экономики в целом. В результате спрос на разработчиков и специалистов в области технической безопасности, в частности, останется высоким.

Глядя на некоторые конкретные технологии, становится ясно, что переход к облачным вычислениям будет продолжаться, и эта долгосрочная тенденция не показывает признаков замедления. Что может измениться, так это то, что компании станут более аналитическими в отношении своего использования облачных вычислений, на которое приходится все большая часть их расходов.

Поиск способов сделать использование облака более эффективным и экономичным, вероятно, станет ключевым вопросом в следующем году — хотя ИТ-бюджеты будут расти, это не означает, что есть место для потерь. Действительно, отрадно видеть, что устойчивость снова поднимается в повестке дня многих технологических организаций, и мы, вероятно, увидим больше этого в 2023 году и далее.

Эти три тенденции

В 2023 году я с интересом слежу за тремя крупными тенденциями в области потребительских технологий, и именно здесь будут найдены некоторые из самых интересных инноваций. Небольшие шаги в 2023 году могут громко отразиться в последующие годы.

Складные смартфоны существуют уже некоторое время, но остаются крошечной частью общего рынка. Мне все еще нравится идея возможности сложить большой экран и носить его с собой, и есть несколько интересных вариантов использования складных телефонов — вопрос будет заключаться в том, будут ли потребители убеждены расстаться со своими деньгами.

Вторая большая тенденция связана с виртуальной реальностью, дополненной реальностью и метавселенной. Крупные технологии тратят здесь большие деньги, и есть некоторые предположения, что базовые технологии достигают критической точки, даже если более широкие бизнес-модели метавселенной в лучшем случае все еще находятся в движении. Технологии гарнитур начинают объединяться, а программное обеспечение становится проще в использовании. Но самая большая проблема заключается в том, что потребительский интерес и доверие все еще низки, хотя бы потому, что писатели-фантасты давно пришли к этому со своим антиутопическим взглядом на будущее гарнитуры. Завоевание доверия потребителей и объяснение того, почему люди могут захотеть участвовать, является таким же высоким приоритетом, как и сама технология.

Одна технологическая тенденция, которая, возможно, ближе, хотя мы ее и не видим, — это окружающие вычисления. Эта концепция существует уже несколько десятилетий: идея состоит в том, что нам не нужно носить с собой технологии, потому что интеллект встроен в окружающий нас мир, от умных колонок до умных домов. Окружающие вычисления предназначены для того, чтобы исчезать в окружающей нас среде — возможно, поэтому эта тенденция оставалась невидимой для многих, по крайней мере, до сих пор.

В некотором смысле долгосрочные прогнозы легче делать, чем краткосрочные, особенно когда речь идет о технологиях. Мы знаем общее направление движения, мы просто не знаем, когда мы на самом деле туда доберемся. До некоторых прорывов оставалось пять лет на протяжении десятилетий — возможно, 2023 год станет годом, когда некоторые из них действительно начнут происходить». ***(Steve Ranger. Three tech trends on the verge of a breakthrough in 2023 // ZDNET (https://www.zdnet.com/article/three-tech-trends-on-the-verge-of-a-breakthrough-in-2023/). 20.11.2022).***

***

«Вот что, по мнению экспертов, будет главными технологическими трендами на 2023 год.

Руководители технологических компаний ожидают, что их бюджеты на технологии вырастут в следующем году, согласно прогнозам аналитиков и других опросов, несмотря на экономические трудности. ZDNET поговорил с техническими руководителями и инсайдерами отрасли, чтобы узнать, поскольку расходы продолжают расти, где лидеры цифровых технологий рассчитывают расставить приоритеты для своих инвестиций в 2023 году.

1. Использование облака в качестве основы для машинного обучения

Барри Панайи (Barry Panayi), директор по данным и аналитике John Lewis Partnership, считает, что в следующем году основной тенденцией в большинстве традиционных предприятий будет получение максимальной отдачи от облака.

«Это разговор 10-летней давности. До сих пор многие люди относились к облаку как к огромному жесткому диску, но оно дает вам огромные возможности», — говорит он.

Панайи говорит, что одним из примеров является то, как компании могут создать значительную ценность, используя данные, хранящиеся в облаке, в качестве основы для MLOps, целью которого является повышение эффективности рабочих процессов машинного обучения в организации.

«Правильные, автоматизированные MLOps — безусловно, в розничной торговле и товарах повседневного спроса — могут изменить правила игры, особенно когда люди все больше совершают покупки в Интернете. Мы известны своими магазинами John Lewis, но сдвиг в Интернете был настолько значительным, что все, что связано с перемещением данных в близком или реальном времени, имеет для нас большое значение».

2. Будьте готовы к метавселенной

Лиза Хенеган, глобальный директор по цифровым технологиям консалтинговой компании KPMG, признает, что метавселенная переоценена. Тем не

менее, она также считает, что бизнес-лидеры должны будут начать осваивать эту быстро развивающуюся область технологий в 2023 году.

«В каком-то смысле я ненавижу говорить, что метавселенная станет следующей большой тенденцией, и я не думаю, что метавселенная и Web 3.0 воплотятся в жизнь в следующем году. Но я действительно думаю, что нам нужно изменить то, как мы думаем, чтобы понять, как изменится мир в течение следующих пяти лет».

Хенеган говорит, что смотрит на то, как молодые люди уже привыкли к все более захватывающему опыту, и предлагает компаниям сейчас разобраться с метавселенной — то, что многие не смогли сделать в прошлом с другими крупными тенденциями.

«Я помню, когда пришло облако, и все спрашивали: «Что такое облако?» Мы не можем ждать столько времени, сколько потребовалось, чтобы все заработало с облаком. С метавселенной мы должны действовать сообща. Мы должны понять ее, начать тестировать и посмотреть, как эта технология может изменить нас».

3. Обеспечение надежности и объяснимости данных

Дэвид Чарнли, глава отдела трансформации и стратегии NatWest, указывает на ряд ключевых проблем, связанных с данными, таких как открытое банковское обслуживание, искусственный интеллект и регулирование: «Все это важные тенденции и действия, за которыми нам нужно очень внимательно следить. на."

Чарнли говорит, что еще одной ключевой проблемой является спрос на таланты, особенно когда такие компании, как его, пытаются расширить свои практики работы с данными: «Я думаю, что тенденция, которую мы наблюдаем, — это нехватка специалистов по данным на рынке труда, и я вижу, что это становится только жестче. Я думаю, что это особенность рынка Великобритании, рынка Индии и других стран».

По словам Чарнли, поскольку его банк продолжает стремиться делать интересные вещи с информацией, которую он хранит, также важно следить за этикой данных и потенциальной предвзятостью. Он признает, что модели машинного обучения могут иметь непреднамеренную предвзятость, и решение этих проблем станет большим приоритетом на 2023 год.

«Достижение того, чтобы мы могли объяснять и отслеживать модели, чтобы гарантировать отсутствие дрейфа или предвзятости в том, как мы ведем бизнес, является частью предоставления отличных предложений по данным. И это то, во что мы действительно инвестируем. время и усилия прямо сейчас в NatWest».

4. Получение максимальной отдачи от облака

Бев Уайт, генеральный директор рекрутерской компании Nash Squared, является еще одним экспертом, который говорит, что главным приоритетом для большинства цифровых руководителей будет получение максимальной отдачи от своих инвестиций в облако.

«В этом нет никаких сомнений, — говорит она. «Поговорите с любым технологическим руководителем, и он будет говорить об этом в первую или вторую очередь. Каждый раз именно сюда они вкладывают свои большие инвестиции — и они будут продолжать делать это в течение следующих нескольких лет».

Уайт говорит, что эти инвестиции в облако будут поддерживаться обязательствами по инвестициям в кибербезопасность.

«Чем более уязвимыми мы делаем наш бизнес в Интернете, тем больше мы рискуем», — говорит она. «И, хотя каждую неделю мы слышим о множестве примеров киберпреступлений, программ-вымогателей и обо всех других вещах, которые происходят, я уверен, что мы мало слышим о многих атаках. Итак, мы ожидаем, что требование инвестировать больше в кибер, чтобы продолжать».

5. Решение проблем кибербезопасности

Сильный акцент на упреждающие и превентивные кибермеры — это то, что перекликается с Энди Пококом, ИТ-директором TrustFord, который говорит, что его приоритет прост: обеспечение безопасности и защиты данных.

«Я думаю, что большой тенденцией будет безопасность и решение этой проблемы. Я, безусловно, в центре внимания. Просто убедиться, что у меня есть возможности и средства защиты для защиты данных моей компании и данных моих клиентов», — говорит он.

«Вам нужно только пойти и прочитать Национальную киберстратегию, и вам нужно только послушать Национальный центр кибербезопасности. Киберугроза постоянно развивается, и она будет становиться все больше».

6. Использование Интернета вещей для контроля

Эд Хиггс, директор группы общих ИТ-сервисов компании Rentokil Initial, специализирующейся на борьбе с вредителями, говорит, что его организация будет стремиться использовать Интернет вещей (IoT) и данные с подключенных устройств.

Его компания использует ловушки, подключенные к Интернету вещей, для автоматического обнаружения признаков заражения, что позволяет бизнесу принимать незамедлительные профилактические меры до того, как проблема усугубится.

«У нас есть миллионы подключенных устройств. Для нас это будет больше IoT, гораздо больше контроля над этой конечной точкой и гораздо больше функций, связанных с этой конечной точкой», — говорит Хиггс.

«Мы перешли от простого наличия SIM-карты в устройстве, которое отправляет SMS, к добавлению камеры к устройству, так что, когда оно отправляет SMS, оно также может отправлять подробную информацию о том, что они сделали. Таким образом, управление, безопасность и соответствие этим конечным устройствам будут иметь для нас большое значение». ***(Mark Samuels. Tech in 2023: 6 new priorities for your shortlist // ZDNET (https://www.zdnet.com/article/technology-spending-will-rise-next-year-and-this-old-favourite-is-still-a-top-priority/). 22.11.2022).***

***

«В этом интервью для Help net Security Брэд Джонс, вице-президент по информационной безопасности Seagate Technology, рассказывает о тенденциях кибербезопасности, с которыми организации столкнутся в ближайшее время, особенно о неправильной конфигурации облака, классификации данных, уязвимостях программного обеспечения и пробелах в навыках кибербезопасности.

Риски кибербезопасности — постоянно развивающаяся проблема для всех организаций. С какими основными из них мы будем иметь дело в ближайшем будущем?

Особое внимание будет уделено неправильной конфигурации облака. Он уже завоевывает позиции в качестве основного источника утечек данных и не собирается сдаваться. В традиционной локальной среде хранения данных только несколько членов группы безопасности контролировали брандмауэр, который не позволял злоумышленникам раскрывать конфиденциальную информацию и предотвращал случайное раскрытие данных сотрудниками.

Однако по мере того, как мир трансформируется и мультиоблачное хранилище становится все более распространенным, проблемы безопасности становятся все более сложными. Компании без ограждений и руководств по управлению доступом подвергают себя риску. Они должны уделять первоочередное внимание соответствию во всей облачной инфраструктуре. Любые ошибки или пробелы в конфигурации облака означают, что любой сотрудник может быть в одном щелчке мыши от случайного раскрытия целых баз данных. Как только информация становится общедоступной, чрезвычайно трудно предотвратить использование злоумышленниками ее в гнусных целях.

Компаниям необходимо обеспечить безопасность с самого начала перехода к облаку, потому что модернизировать основу безопасности гораздо сложнее. Если компания не решает проблему безопасности в облаке, то она просто переносит плохие практики из одного облака в другое при переходе на мультиоблако. Управление идентификацией и доступом, автоматизация облачной конфигурации и внедрение нулевого доверия могут помочь обеспечить соответствие требованиям в мультиоблачной среде.

Какие изменения вы видите в классификации данных?

Классификация данных сильно различается по категориям (PII, здравоохранение, финансы и т. д.), поскольку каждый тип данных регулируется по-разному в зависимости от отрасли и местоположения. Если у организации нет единой стратегии классификации, она становится открытой для злоумышленников, желающих нажиться на ценных данных, а также крупных штрафов от регулирующих органов, если сотрудники случайно неправильно обращаются с данными. Чтобы избежать этого, компании будут создавать способы для более тесного сотрудничества между своими группами безопасности и отделами, которые обрабатывают конфиденциальные данные.

Разработка всеобъемлющей системы классификации данных сложна, и специалисты по безопасности не могут справиться с ней в одиночку. Классификация данных требует ввода и соблюдения со стороны всей организации. Правила конфиденциальности и безопасности данных будут становиться все более сложными, а финансовые последствия их несоблюдения станут более серьезными. В результате мы увидим, как юридические отделы, команды безопасности и владельцы данных из других отделов будут работать вместе, чтобы классифицировать, управлять и защищать ценные данные.

Поскольку уязвимости программного обеспечения выходят на первый план, как поставщики программного обеспечения должны реагировать?

В 2023 году поставщики программного обеспечения должны использовать прозрачный и коммуникативный подход, чтобы завоевать больше доверия клиентов. Клиенты все больше беспокоятся о безопасности. Ранее в этом году федеральным указом было введено более жесткое регулирование для поставщиков программного обеспечения и услуг, чтобы они были более прозрачными в отношении потенциальных киберугроз и рисков, в дополнение к реальным киберинцидентам, с которыми они могут столкнуться.

Забота о клиентах и федеральное регулирование означают, что поставщики программного обеспечения и услуг должны быть более прозрачными в отношении того, что в их стеках технологий может иметь последствия для безопасности в будущем. Поставщики должны будут открыто сообщать о том, что находится в их спецификации программного обеспечения (SBOM), если, например, они используют Log4J или Java или другое программное обеспечение в своей среде. SBOM — это перечень программного обеспечения и компонентов, из которых состоит приложение.

Знание этих деталей позволяет организациям принимать более обоснованные решения при выборе поставщиков, поэтому они могут избегать программного обеспечения, которое может привести к угрозам безопасности. Поставщики, которые более прозрачны в отношении своих технологических стеков, будут лучше подготовлены к проверке со стороны клиентов и регулирующих органов в случае киберугрозы.

Мы уже давно слышим о пробеле в навыках кибербезопасности. Как вы думаете, что может быть решением этой проблемы?

С меньшим количеством квалифицированных работников компании растягивают имеющийся персонал, чтобы охватить несколько областей. Однако эксперт по брандмауэрам не может за одну ночь стать экспертом по безопасности облачных вычислений, а один ИТ-специалист не может знать все тонкости каждой облачной среды. Чтобы решить проблему нехватки кадров, компании все чаще обращаются к автоматизированным инструментам безопасности, которые облегчают работу сотрудников и обеспечивают экономию средств. Однако управление этими инструментами по-прежнему требует специальных навыков.

Автоматизация устраняет существующий пробел в навыках безопасности, но в будущем он создаст еще один, поскольку компаниям потребуется все больше и больше сотрудников с опытом автоматизации. Долгосрочное решение для преодоления разрыва в навыках — это стратегическое внедрение новых технологий и повышение квалификации ИТ-персонала. Например, обучая специалистов по безопасности управлению автоматизированными инструментами безопасности, не зависящими от облака, компании могут лучше управлять безопасностью в мультиоблачной среде.

Существуют ли какие-либо другие тенденции в области кибербезопасности, о которых следует знать организациям?

Правила безопасности стимулируют тенденцию к локализации данных, к которой ИТ-руководители должны быть готовы прямо сейчас. Когда дело доходит до локализации данных, действуют два основных фактора: распространение периферийных устройств и быстро меняющееся государственное законодательство,

определяющее, как компании хранят и используют свои данные. Поскольку компании хранят больше информации на периферии, у них больше потребностей в локализованном хранении и безопасности.

Поскольку все больше данных локализуется, все больше компаний должны соблюдать региональные правила конфиденциальности данных, такие как GDPR и Закон о защите прав потребителей штата Калифорния (CCPA). Региональные нормативные акты затрудняют для компаний удовлетворение своих потребностей в хранении данных с помощью одного облака, что потребует более широкого внедрения нескольких облаков. Большему количеству компаний потребуются разные облака в разных регионах для выполнения разных задач. По мере того, как они вступают на путь мультиоблака, компаниям потребуется четкая основа безопасности, чтобы избежать неправильной настройки облака, которая подвергает риску многие организации». ***(Helga Labus. The cybersecurity trends organizations will soon be dealing with // Help Net Security (https://www.helpnetsecurity.com/2022/11/29/cybersecurity-trends/). 29.11.2022).***

***

«Во всем мире компании испытывают финансовые затруднения. В США инфляция выросла до 8,2% в сентябре 2022 г., а Федеральная резервная система повысила процентные ставки до диапазона 3–3,25%, что является самым высоким показателем с 2008 г. Поскольку организации все больше опасаются перспективы рецессии и ощущают влияние роста цены, инвестиции тщательно изучаются, а расходы утверждаются только по самым важным причинам. В этих условиях ИТ-специалистам и специалистам по кибербезопасности необходимо подумать о том, как они могут обеспечить постоянную эффективность бизнеса и снизить риск взлома, демонстрируя при этом окупаемость инвестиций в свои расходы на безопасность. В настоящее время команды корпоративной безопасности борются с в среднем 76 инструментами безопасности., ответ заключается не просто в добавлении большего количества точечных решений. Вместо этого оптимизация существующих инструментов и обеспечение их эффективного развертывания и работы помогает снизить сложность, высвободить ресурсы и обеспечить более эффективное распределение бюджета.

Почему меньше значит больше

Меняется отношение к расходам на кибербезопасность: в отчете PwC Global Digital Trust Insights за 2022 год говорится, что 69% организаций прогнозируют рост расходов на кибербезопасность в 2022 году по сравнению с 55% в прошлом году. Однако большие расходы не означают лучшей безопасности или большей согласованности между безопасностью и бизнес-стратегией. Фактически, в своем стремлении к большему финансированию и инструментам кибербезопасности организации пренебрегают основным принципом безопасности. Сложная система, состоящая из бесчисленных инструментов, предоставляет командам безопасности больше данных для анализа и повышает вероятность сбоев в управлении. В свою очередь, это увеличивает нагрузку на и без того перегруженных специалистов по безопасности, которые борются с нехваткой рабочей силы, составляющей более 2,72 миллиона должностей.

Вместо этого вы хотите согласиться с идеей, что меньше значит больше. Стремясь упростить общую стратегию безопасности и сосредоточив внимание на эффективности и результативности, организации могут максимально использовать то, что у них уже есть. Затем ресурсы могут быть распределены по приоритетам в областях, которые оказывают наибольшее влияние на безопасность и быстро снижают риск.

Стремление к тому, чтобы меньше значит больше, также помогает бороться с восприятием безопасности как обременительного центра затрат. ИТ-специалисты и специалисты по безопасности могут столкнуться с трудностями при доведении информации о возврате инвестиций (ROI) до совета директоров, который слишком часто распределяет бюджет безопасности реактивным образом. Этот подход должен измениться.

Учитывая, что члены совета директоров более позитивно реагируют на конкретные факты, чем на «если» и «может быть», директорам по информационной безопасности и их командам необходимо продемонстрировать финансовые преимущества проактивной и разумной кибербезопасности при одновременном снижении рисков и повышении эффективности.

Как сделать больше за меньшие деньги

На практике делать больше за меньшие деньги означает смотреть внутрь себя — на свой бизнес и стратегию безопасности, на используемые в настоящее время инструменты безопасности и на культуру вашей компании — и оптимизировать их там, где это возможно.

1. Оптимизация кибербезопасности и ИТ-операций

При оценке существующего стека безопасности необходимо задать несколько важных вопросов: Получаете ли вы максимальную отдачу от своих инструментов? Как вы измеряете их эффективность и результативность? Какие-то инструменты бездействуют? И насколько достигается автоматизация?

То же самое следует спросить о вашем ИТ-стеке — есть ли раздувание и технический долг? В вашей ИТ-инфраструктуре и инфраструктуре безопасности часто присутствуют ненужные уровни сложности процессов, политик и инструментов, которые могут привести к потерям. Например, наличие слишком большого количества инструментов приводит к высоким накладным расходам на обслуживание и настройку, что истощает как ресурсы, так и деньги. Точно так же технологии, сочетающие локальную инфраструктуру и сторонних облачных провайдеров, требуют сложного управления и процессов.

Поэтому ИТ-специалистам и специалистам по кибербезопасности необходимо работать вместе, руководствуясь четким общим видением, чтобы найти способы повышения эффективности без снижения уровня безопасности. Это требует ясности в отношении ролей и обязанностей между службами безопасности и ИТ-отделами для управления активами и развертывания инструментов безопасности. Звучит просто, но часто это не так из-за исторических подходов к внедрению инструментов.

Если команды могут получить ясность в отношении общих приоритетов за счет большей прозрачности активов и технологий, это окажет большое влияние на совместную работу и производительность.

2. Автоматизация в приоритете

Центральным элементом, позволяющим делать больше при меньших затратах на практике, является автоматизация. Например, автоматизация ключевых областей, таких как управление активами и средствами контроля безопасности, дает директорам по информационной безопасности и их командам четкое представление об их инвентаризации активов, что имеет решающее значение в эпоху удаленной работы и ожиданий гибкости. Это также способствует пониманию состояния и эффективности мер безопасности с помощью метрик и измерений.

Одним из все более популярных решений является мониторинг непрерывного контроля (CCM). Сопоставляя данные из всех источников безопасности и соответствующих бизнес-источников, CCM выявляет отсутствующие активы и пробелы в защите, улучшает совместную работу и расстановку приоритетов, оптимизирует элементы управления безопасностью и автоматизирует рабочие процессы исправления, чтобы помочь организациям максимально эффективно использовать существующие инвестиции в безопасность.

Заглядывая вперед

С коммерциализацией наступательных наборов инструментов кибербезопасности и новых бизнес-моделей для злоумышленников риск кибератак никуда не делся. Большинство взломов происходит из-за сбоя средств защиты, когда у организации были инструменты, необходимые для предотвращения или смягчения атаки, но они не были правильно развернуты. Мы рекомендуем вернуться к основам, проверить имеющиеся у них элементы управления и убедиться, что они работают должным образом на всех ресурсах, чтобы избежать предотвратимого нарушения.

Будь то технический долг и сложность бизнеса, разрастание инструментов или разрозненная культура безопасности, которые требуют решения, всегда есть возможности для оптимизации. А благодаря таким решениям, как CCM, автоматизация может помочь командам сэкономить деньги и ресурсы, одновременно снизив риски кибербезопасности». ***(Nick Lines. Cybersecurity: How to do More for Less // Techstrong Group Inc. (https://securityboulevard.com/2022/11/cybersecurity-how-to-do-more-for-less/). 29.11.2022).***

***

«Вы остаетесь впереди или отстаете от кривой кибербезопасности?

Адаптивный контроль, отсутствие доверия, нулевое доверие, искусственный интеллект с автоматическим исправлением и фильтр содержимого с многофакторной аутентификацией, согласующийся с вашим развертыванием CASB, добавляет технологию с открытым исходным кодом, неисправленную критическую инфраструктуру, защищены ли риски кибербезопасности вашей организации и требования соответствия?

Оставаться впереди угроз или не реагировать на растущую скорость атаки по-прежнему является 800-фунтовой гориллой в каждой виртуальной комнате и на собрании в масштабе.

«Мы более безопасны, потому что мы установили «X», и мы соблюдаем требования, потому что мы наняли «Y» в качестве нашего MSSP для поддержки нашей стратегии XDR?»

Скорее всего, ответ может быть категорическим нет.

Наблюдая за тем, как клиенты в течение 28 лет развертывают новейшие, наиболее важные автоматизированные компоненты с компонентом управляемых услуг для решения нескольких проблем, я еще не видел ожидаемых ими результатов, а также наблюдаю, как текущие расходы на обеспечение безопасности превышают заранее установленную цифру бюджета.

Хакеры, фишеры, киберпреступники, внутренние злоумышленники и имитаторы цепочки поставок продолжают добиваться большего успеха в своих фишинговых атаках по электронной почте. BEC, похищающий данные изнутри и ставящий под угрозу критически важные системы, тихо удаляющийся в течение последних трех месяцев, продолжает расти во всем мире.

Время для новой перспективы? Абсолютно.

Перемещение виртуальных ворот

Директорам по информационной безопасности, ИТ-директорам и финансовым директорам следует взять на себя оставшуюся часть четвертого квартала 2022 года, чтобы подумать о том, как организация может изменить свою стратегию безопасности на 2023 год и скорректировать свои «целевые показатели».

Прогнозируя последующее нарушение кибербезопасности, атаку нулевого дня или обнаружение сотрудников, уходящих с ценной интеллектуальной собственностью, как организация может перестроить свои ожидания в отношении SecOps, DevOps, DevSecOps, AIOps и CloudOps в новом году?

Сначала используйте подход, основанный на оценке рисков.

Атаки на кибербезопасность в 2022 и 2023 годах будут по-прежнему влиять на бренды организаций, прибыль и сотрудников. Команды SecOps и их партнеры в DevOps и CloudOps борются с проигранной игрой на истощение, особенно с проблемами безопасности продукта.

Нарушения кибербезопасности останутся проблемой и в 2023 году. Выгорание сотрудников приведет к человеческим и общесистемным ошибкам, созданию уязвимостей и эксплойтов. Снижение риска человеческого капитала и обеспечение лучших условий работы для команд безопасности поможет защитить организацию.

Застраховать риск — это решающий фактор для решений цифровой трансформации.

Большинство стратегий цифровой трансформации терпят неудачу из-за кибератаки или наличия неуправляемой модели операций после развертывания с новыми прорывными технологиями.

Организация должна иметь ресурсы для поддержания всех средств управления операциями безопасности, процессов и случаев реагирования на инциденты. Организациям требуется больше ресурсов для поддержки мероприятий по обеспечению безопасности. Наличие риска в качестве основного компонента принятия организацией решения о стратегии преобразования может быть эффективной стратегией снижения риска.

Для снижения риска организации требуется нечто большее, чем масштабирование за пределы адекватных возможностей защиты данных.

Делайте ставку на все следующего поколения

Часто организации разрабатывают свои стратегии преобразования на основе усовершенствованных или даже революционных технологических возможностей, в

том числе технологий, меняющих мир, таких как доступ без пароля для закрепления своей системы. Да, многие технологические достижения, в том числе коммуникационная платформа как услуга (Cpaas) и принцип нулевого доверия, открывают большие перспективы в преобразовании технологических возможностей бизнеса за счет повышения уровня интегрированной безопасности.

Однако все технологии будут иметь уязвимости, приводящие к увеличению количества атак и киберугроз, независимо от того, какой поставщик разработал решение. В конечном счете, если якорная технология выйдет из строя или будет скомпрометирована, будет ли влияние на организацию меньше, чем стоимость стратегии трансформации, или больше? Для определения потенциального воздействия на организацию требуется простая оценка рисков, включая участие красно-синих команд и развертывание платформы управления нормативными рисками.

Вывод

Скорость атак кибербезопасности будет продолжать расти. Потенциальные уязвимости всегда будут существовать.

MSSP, адаптивный ИИ и XDR — это возможности, а не решения. Люди — это решение. У сотрудников есть способности и опыт, как правильно использовать эти возможности. Доверьтесь им.

Опыт сотрудников защищает пользовательский опыт.

Люди стоят вложений в снижение организационных рисков». ***(John P. Gormally. Moving the Cybersecurity Goal Posts // Techstrong Group Inc. (https://securityboulevard.com/2022/11/moving-the-cybersecurity-goal-posts/). 28.11.2022).***

***

«Barrier Networks объявила о начале нового партнерства с Zurich Resilience Solutions, частью Zurich UK, чтобы предлагать предприятиям технические услуги в области кибербезопасности, чтобы помочь им повысить свою киберустойчивость.

Киберпреступность — это вызов, с которым сегодня сталкиваются все организации, и ключевым элементом их защиты является киберстрахование. Эти политики позволяют компаниям компенсировать финансовые потери, вызванные атаками, и компенсировать расходы третьих сторон, связанные с нарушениями безопасности, но для получения покрытия они должны применять передовые методы обеспечения безопасности и демонстрировать киберустойчивость.

Zurich Resilience Solutions (ZRS) предоставляет андеррайтерам страховые гарантии, чтобы помочь им лучше понять кибер-риски и подверженность клиентских сред, а также предоставляет клиентам консультационные услуги по кибер-рискам и устойчивости для повышения кибер-устойчивости.

Barrier Networks дополняет внутренние консультационные услуги ZRS по киберрискам, предлагая техническую экспертизу и услуги, включая тестирование на проникновение, управляемые услуги по кибербезопасности, оценку и консультации.

Говоря о партнерстве, Ян МакГоуэн, управляющий директор Barrier Networks, выразил радость от сотрудничества с Цюрихом и считает, что партнерство поможет многим организациям улучшить свою кибербезопасность.

«Мы рады работать с таким признанным игроком в области киберстрахования, как Цюрих», — сказал Макгоуэн. «Кибербезопасность — это огромная задача для большинства предприятий, и очень немногие имеют ресурсы, чтобы справиться с ней в одиночку.

«Наше партнерство поможет организациям преодолеть эту проблему, поскольку мы помогаем им улучшить их безопасность и решить ключевые проблемы для удовлетворения критических требований киберстрахования.

«Сегодня ни одна организация не может рисковать своей киберзащитой, и благодаря нашему партнерству мы будем вооружать больше предприятий навыками и опытом, необходимыми им для обеспечения безопасности».

Партнерство будет сосредоточено не только на корпоративной безопасности, но и на организациях, использующих операционные технологии в критически важных промышленных средах.

В последнее время эти организации подвергаются повышенной угрозе со стороны киберпреступности, и Barrier Networks и Zurich помогут удовлетворить эти потребности, помогая им снизить риск утечки данных, которая может быть вызвана неизвестными проблемами кибербезопасности.

Добавляя дополнительные комментарии, Арунава Банерджи, руководитель отдела консультирования по вопросам киберрисков в Zurich Resilience Solutions, сказала, что партнерство является огромным стимулом, учитывая характер киберрисков в настоящее время.

«Это партнерство еще больше укрепит набор консультационных услуг по киберрискам, которые мы предлагаем клиентам», — сказал Банерджи. «Киберриск — это серьезная угроза, с которой сталкиваются компании любого размера.

«Укрепляя их киберзащиту, мы можем помочь компаниям уменьшить свою подверженность атакам и лучше ориентироваться на нынешнем жестком рынке страхового покрытия». ***(Zoe Deighton Smythe. Zurich partners with Barrier Networks to offer enterprise Cyber Risk Assessments // Security on Screen (https://securityonscreen.com/zurich-partners-with-barrier-networks-to-offer-enterprise-cyber-risk-assessments/). 24.11.2022).***

***

«AmiViz объявила о заключении стратегического альянса с базирующейся в Саудовской Аравии CyberME Studio, независимой венчурной студией, которая занимается выявлением, инвестированием, развитием, запуском и продвижением саудовских стартапов, ориентированных исключительно на решения в области кибербезопасности.

Обе компании вместе выставляются на выставке Black Hat MEA в Эр-Рияде с 15 по 17 ноября 2022 года, и на выставке AmiViz представляет CyberME Studio и ее ассоциированные компании; Cognna, Kensa и 2FAST.

Говоря об альянсе, Ильяс Мохамед, главный операционный директор AmiViz, выразил свое восхищение CyberME Studio и считает, что партнерство с компанией

свидетельствует о значительном росте AmiViz, особенно с учетом того, что это их первое решение, посвященное решениям для Саудовской Аравии.

«CyberME Studio проделывает потрясающую работу, и стартапы под ее руководством разработали решения для кибербезопасности мирового класса», — сказал Мохамед. «Мы очень рады представить их портфолио и продемонстрировать свои решения на выставке Black Hat.

«CyberME Studio — это единственное в своем роде предприятие в Саудовской Аравии, которое занимается разработкой технологий в области кибербезопасности для решения проблем, с которыми сталкиваются клиенты в современную эпоху. Из нашего большого портфолио это наше первое партнерство, представляющее саудовские технологии кибербезопасности».

CyberME Studio ставит перед собой задачу вывести Саудовскую Аравию в число стран, способных запускать собственные компании в области кибербезопасности, чтобы обслуживать клиентов по всему миру и обслуживать мировой рынок кибербезопасности стоимостью 300 миллиардов долларов США.

Альянс завершает отличный год для компании, которая также смогла успешно запустить несколько новых стартапов, включая Cognna, Kensa и 2FAST в прошлом году.

CyberME Studio продвигает эти компании на различных форумах и выставках. Компания участвовала в LEAP 2021, @hack 2021 и Global Entrepreneurship Congress 2022, а теперь благодаря стратегическому партнерству с AmiViz CyberME Studio решила принять участие в Black Hat 2022 в Эр-Рияде.

Выразив свое восхищение партнерством с AmiViz и участием в Black Hat, Абдулрахман Баджабер, генеральный директор CyberME Studio, сказал, что альянс стал вишенкой на торте блестящего года, и что ему не терпится увидеть, какое влияние они могут оказать. на глобусе.

«Мы в восторге от результатов всех этих трех стартапов, которые сосредоточены на другой нише в области кибербезопасности и предлагают решения, которые помогают предприятиям повысить уровень своей безопасности и защитить себя от современных кибератак», — сказал Баджабер.

«Мы в CyberME гордимся тем, что привлекаем лучших людей для создания новой отрасли и распространения ее по всему миру!». ***(Christian Brown. AmiViz and CyberME Studio showcase cybersecurity solutions at Black Hat MEA // Security on Screen (https://securityonscreen.com/amiviz-and-cyberme-studio-showcase-cybersecurity-solutions-at-black-hat-mea/). 15.11.2022).***

***

«Поскольку каждый день появляются новые субъекты угроз, кибербезопасность стала важнейшим требованием бизнеса. Лидеры в области безопасности должны оставаться конкурентоспособными в быстро развивающемся бизнес-ландшафте, а также защищаться от угроз, снижать сложность и способствовать цифровой трансформации.

Чтобы лучше понять главные опасения директоров по информационной безопасности, Microsoft Security провела опрос о киберустойчивости. Продолжайте читать, чтобы узнать о наших результатах.

Примите уязвимость гибридной работы и повысьте устойчивость

Гибридная работа вынудила предприятия всех типов перейти в облако. В результате 61% руководителей в области безопасности заявили, что считают облако цифровым инструментом, наиболее уязвимым для атак, а двое из трех считают, что гибридная работа сделала их организации менее безопасными.

Это беспокойство небезосновательно, учитывая, что 40% всех атак в 2021 году и половина всех облачных атак оказали существенное влияние на бизнес. Исследование Microsoft показало, что нарушения безопасности из-за неправильной настройки облака так же распространены, как и атаки вредоносных программ, и даже в большей степени связаны со значительным ущербом для бизнеса.

Защита облака отличается от защиты внутренней сети и часто может быть сложной задачей. Мы рекомендуем привлекать специалистов по облачной безопасности, чтобы избежать ошибок администратора, таких как неправильная конфигурация и непоследовательная реализация политик безопасности.

Ограничьте воздействие программ-вымогателей

В 2021 году каждая пятая компания подверглась атаке программ -вымогателей, и примерно треть руководителей служб безопасности назвали программы-вымогатели своей главной проблемой. И хотя финансовые аспекты программ-вымогателей разрушительны, они являются лишь частью дела. Около 48 % жертв атак программ-вымогателей, участвовавших в нашем исследовании, сообщили, что атаки привели к значительным простоям в работе, раскрытию конфиденциальных данных и ущербу для репутации.

Атаки программ-вымогателей сводятся к трем основным векторам входа: грубой силе протокола удаленного рабочего стола (RDP), уязвимым системам с выходом в Интернет и фишингу. Организации могут ограничить ущерб, заставив злоумышленников усерднее работать, чтобы получить доступ к нескольким критически важным для бизнеса системам. Принципы нулевого доверия, такие как доступ с наименьшими привилегиями, особенно эффективны для предотвращения распространения атак по сети и борьбы с программами-вымогателями, управляемыми людьми.

Превратите кибербезопасность в стратегическую бизнес-функцию

Среди директоров по информационной безопасности происходит интересное изменение мышления: надежная система безопасности должна быть направлена на повышение осведомленности о ландшафте угроз и создании устойчивости, а не на предотвращении отдельных атак.

Данные опроса Microsoft подтверждают эту точку зрения; 98 % респондентов, которые сообщили, что чувствуют себя крайне уязвимыми для атак, также внедряли нулевое доверие, а 78 % уже применяли комплексную стратегию нулевого доверия. Поскольку нулевое доверие предполагает нарушение и оптимизируется для устойчивости, а не для защиты, респонденты, которые указали на зрелость в своем пути к нулевому доверию, также с большей вероятностью рассматривали атаки как неизбежную, а не предотвратимую угрозу. И хотя реализация нулевого доверия не обязательно приводит к меньшему количеству атак, она может помочь снизить среднюю стоимость взлома.

Максимизируйте свои существующие ресурсы

Хотя эти данные могут показаться ужасными, многие директора по информационной безопасности также с оптимизмом смотрят на свою способность справляться с будущими проблемами в будущем.

Например, почти 60% руководителей заявили, что сегодня считают сети уязвимостью. Тем не менее, только 40% считают, что проблема не исчезнет через два года. Аналогичным образом, электронная почта, инструменты для совместной работы и конечные пользователи в качестве ожидаемых проблем в 2024 году упоминаются на 26 % меньше, чем в 2022 году, и примерно на 20 % меньше считают уязвимость цепочки поставок главной проблемой. Ожидается, что через два года только операционные технологии (OT) и Интернет вещей (IoT) станут такой же или более сложной задачей.

Опираясь на прочную основу с нулевым доверием, организации могут оптимизировать свои инвестиции в безопасность, такие как обнаружение конечных точек и реагирование на них, безопасность электронной почты, управление идентификацией и доступом, брокер безопасности облачного доступа и встроенные инструменты защиты от угроз.

Внедрение основ безопасности

Сегодня директоров по информационной безопасности просят делать больше с меньшими затратами. Лидеры в области безопасности должны максимально эффективно использовать имеющиеся у них ресурсы, расставив правильные приоритеты, начиная с основополагающих передовых практик в области кибербезопасности.

По оценкам Microsoft, 98 % кибератак можно предотвратить с помощью базовых правил безопасности, таких как многофакторная проверка подлинности (MFA), доступ с минимальными привилегиями, регулярные обновления программного обеспечения, защита от вредоносных программ и защита данных. Тем не менее, по состоянию на декабрь 2021 года только 22% клиентов, использующих облачное решение Microsoft для идентификации, Azure Active Directory, внедрили надежную защиту аутентификации.

Повышение вашей киберустойчивости не происходит в одночасье. Это непрерывный путь, в котором находятся все организации, поскольку мы продвигаемся вперед в этой быстро меняющейся среде угроз. Расставляя приоритеты, на что необходимо обратить внимание в первую очередь, в зависимости от риска, организации могут постепенно применять эти пять шагов, чтобы уверенно двигаться к повышению киберустойчивости». ***(Security Leaders Share 5 Steps to Strengthen Cyber Resilience // Informa PLC Informa UK Limited (https://www.darkreading.com/microsoft/security-leaders-share-5-steps-to-strengthen-cyber-resilience). 03.11.2022).***

***

«…В связи с ростом количества модификаций современных компьютерных вирусов и видов атак, специалисты по информационной безопасности выделяет различные тренды кибербезопасности. Защита сайта от DDoS атак — одна из важнейших задач владельца бизнеса. АО «Казтелепорт» в Казахстане предлагает услугу надежной защиты серверов от DDoS. Специалисты

компании детально анализируют IT-инфраструктуру, изучают ее специфику и особенности, чтобы обеспечить наиболее эффективную защиту информации клиентов. Детальнее об услуге, читайте здесь.

Рассмотрим другие современные тенденции защиты от киберугроз.

Облачная платформа защиты приложений (CNAPP)

Внедрение в компании облачной инфраструктуры может спровоцировать дополнительные угрозы конфиденциальности данных. Чтобы обезопасить удаленные среды от действий злоумышленников, провайдеры внедряют следующие решения:

- CWPP — Cloud Workload Protection Platform;
- CSPM — Cloud Security Posture Management;
- CSNS — Cloud Service Network Security.

Гибридная IT-инфраструктура

Гибридные ЦОД вобрали в себя все преимущества облачной и локальной инфраструктур. Такой вариант организации корпоративной сети позволяет хранить важные данные на локальных машинах, а остальную информацию отправлять на облако. Кроме того, удаленные провайдеры предлагают услугу регулярного резервного копирования.

Сам по себе этот способ не предполагает дополнительных защитных мер от хакерских угроз. Однако он позволяет более гибко манипулировать данными и хранить их в разных местах, чтобы в случае утечки не пострадала критически важная информация.

Разделение уровней доступа

При проектировании и создании любого вида IT-инфраструктуры компании нужно обязательно позаботиться о разделении доступа к данным для разных отделов и сотрудников. Иначе, простая халатность или невнимательность работника могут привести к непреднамеренной утечке конфиденциальных данных.

В идеале, у каждого сотрудника должен быть свой собственный корпоративный аккаунт с требуемыми правами доступа. Общедоступную информацию можно хранить на удаленном сервере, в то время как бухгалтерский учет рационально разместить на локальных машинах с регулярным резервным копированием.

Простая архитектура систем безопасности

Часто причиной утечки корпоративных данных может стать сложная и неправильно спроектированная система безопасности. В этом случае количество установленного защитного ПО или аппаратных устройств может сыграть только в худшую сторону. Например, антивирусы, фаерволы и другое ПО могут конфликтовать между собой, что создает дополнительные уязвимости.

Проектированием подобных систем должны заниматься профессиональные специалисты, понимающие какое оборудование и ПО необходимо для реализации поставленных задач.

Профессионализм сотрудников

Часто причиной утечки информации становятся непрофессиональные сотрудники. От этого фактора нельзя защититься ни одной программой. Например, халатный работник может войти в свой корпоративный аккаунт на чужом

компьютере, где сохраняться личные данные, позволяющие злоумышленнику получить несанкционированный доступ.

Поэтому современные предприниматели проводят в компаниях тренинги и внеплановые лекции по увеличению компьютерной грамотности сотрудников. Чтобы обезопасить свой бизнес от интернет-угроз, нужно максимально следовать рекомендациям специалистов по кибербезопасности». ***(5 трендов кибербезопасности в 2022 // Укррудпром (https://ukrrudprom.com/news/5_trendov_kiberbezopasnosti_v_2022.html). 02.11.2022).***

***

«Все більше організацій ставлять кібербезпеку корпоративного середовища одним із пріоритетних завдань для успішної діяльності сьогодні. Забезпечення захисту від атак – серйозний виклик, який залежить від багатьох факторів. У рамках Дня захисту від кіберзагроз спеціалісти ESET підготували список основних викликів, які постають перед кібербезпекою вже зараз та виникнуть у найближчому майбутньому.

1. Збільшення кількості кібератак

Відповідно до звіту Cybersecurity Ventures, очікується, що глобальні збитки, спричинені кіберзлочинною діяльністю зростатимуть на 15% на рік з 2021 до 2025 року та можуть досягти 10,5 трильйонів доларів щорічно. Причинами такого зростання є значний ріст активності груп кіберзлочинців та зловмисників, діяльність яких спонсорується державою. У той же час кількість атак зростає внаслідок процесів цифрової трансформації.

2. Дефіцит кваліфікованих спеціалістів з кібербезпеки

В умовах підвищеного попиту на професіоналів у галузі кібербезпеки продовжує зростати дефіцит кваліфікованих кадрів. Згідно з дослідженням (ISC)2 Cybersecurity Workforce Study, глобальна нестача кадрів у сфері кібербезпеки становить 3,4 мільйона, при цьому 70% організацій мають незакриті вакансії. Багато держав працюють над зменшенням цього дефіциту, а великі компанії, такі як Google, Microsoft або IBM, запроваджують різні ініціативи, спрямовані на навчання та підвищення кваліфікації людей у сфері кібербезпеки.

Тим часом Всесвітній економічний форум спільно з кількома компаніями запустив освітню онлайн-платформу для окремих осіб та організацій під назвою Cybersecurity Learning Hub. Метою цього проекту є навчання та вдосконалення навичок спеціалістів із кібербезпеки для забезпечення якісної роботи в цій галузі.

3. Недостатня підтримка інклюзивного персоналу

На додаток до дефіциту кадрів з’являється інший виклик для кібербезпеки – це підтримка різноманітності та інклюзивності під час вибору персоналу на роботу. Для залучення менш захищених груп суспільства, наприклад, людей з інвалідністю необхідно розробити спеціальні ініціативи та політику.

Це не лише питання цінностей, а й виклик для інновацій та продуктивності, які є ключовими факторами успіху будь-якої організації. Крім цього, залучення таких груп людей допоможе скоротити дефіцит кваліфікованих спеціалістів з кібербезпеки.

4. Перехід на дистанційну та гібридну роботу

У зв'язку із цифровою трансформацією бізнесів, спричиненою пандемією, багато компаній зіткнулися із проблемами у безпеці корпоративного середовища. Тоді кількість спроб атак на протокол віддаленого робочого столу (RDP) зросла на рекордні 768% протягом 2020 року, що виявилось одним із найуразливіших місць в інфраструктурі підприємств.

Тому зараз компаніям варто продовжувати належну підготовку та забезпечення можливостей співробітникам, які працюють віддалено, щоб уникнути потенційних ризиків та захиститися від нових атак кіберзлочинців, які постійно шукають нові недоліки кібербезпеки у корпоративних мережах.

5. Зростання активності у даркнеті

Величезне зростання кримінальної активності у даркнеті за останні роки, особливо після початку пандемії, є серйозною проблемою, яка ще раз показує важливість досліджень у цих мережах Інтернету.

Моніторинг даркнету допомагає спеціалістам з кібербезпеки запобігати атакам, розуміти, як думають шахраї та кіберзлочинці, які шкідливі інструменти використовують зловмисники для доступу до систем організацій або для обману користувачів, а також які корпоративні дані поширюються на чорних ринках.

6. Поява нових витончених тактик кібератак

Одним із різновидів фішингу, який останнім часом активізувався, є гібридний фішинг, який поєднує традиційний метод на основі електронної пошти з вішингом. Цей вид використовується для отримання доступу до систем організації та розгортання шкідливих програм, таких як програми-вимагачі.

Під час нещодавньої атаки потенційна жертва спочатку отримала електронний лист, наприклад, про продовження підписки на послугу. При цьому у разі бажання скасувати підписку користувач може зателефонувати до служби підтримки за номером телефону, вказаним у повідомленні. Під час дзвінка жертву обманом заманюють встановити шкідливу програму, яка часто може поширюватися на інші пристрої.

Тим часом можливості машинного навчання створювати несправжні голоси швидко розвиваються. Серйозною загрозою є кількість атак, під час яких шахраї використовують інструменти на основі машинного навчання. Зокрема для імітації голосу директора певної компанії в режимі реального часу, щоб переконати співробітника переказати гроші на рахунок, який насправді належить зловмисникам.

7. Інтерес до криптовалюти зростає

Не тільки користувачі, компанії та державні установи знаходять нові способи використання криптовалюти, а й кіберзлочинці. Збільшення кількості схем шахрайства з криптовалютою підтвердило інтерес хакерів до цієї галузі. Не дивно, що виклики, пов'язані з безпекою у світі криптовалют, також часто стають заголовками новин.

Використовуючи платформи у галузі криптовалют, NFT та ігор, зловмисники часто створюють нові фішингові сайти для викрадення облікових даних користувачів, зокрема для входу у криптовалютні гаманці. Тоді як криптовалютні біржі потрапляють під приціл APT-груп. Наприклад, нещодавно було викрадено

криптовалюту на суму 625 мільйонів доларів США з відеогри Axie Infinity, що пов'язують із кіберзлочинцями Lazarus.

8. Активність програм-вимагачів все ще висока

Програми-вимагачі все ще залишаються серйозною проблемою, яка вимагає від організацій максимального захисту. Зокрема їм необхідно подбати про інструменти для протидії атакам програм-вимагачів, організацію комплексних навчальних програм з безпеки для співробітників та готовність до відновлення, якщо атака все ж таки трапиться. З 2020 по 2021 рік кількість атак програм-вимагачів зросла удвічі, залишаючись найбільш руйнівною загрозою для підприємств.

9. Вплив віртуального світу

Прогнози щодо розвитку метавсесвіту показують, що до 2026 року 25% населення світу проводитиме принаймні 1 годину на день у цьому віртуальному світі. Тому безпека в метавсесвіті є викликом на майбутнє.

Ці спільні віртуальні світи для спілкування та ігор безсумнівно призведуть до великої кількості атак та шахрайства. Крім того, технологічні інновації не завжди розробляються з урахуванням правил безпеки та конфіденційності, оскільки пріоритетом є швидший вихід на ринок.

10. Недостатня обізнаність користувачів

Базова проблема, з якою кібербезпека завжди стикатиметься, це недостатня цифрова обізнаність працівників щодо векторів атак та способів їх розпізнання. Тому співробітники є найслабшою ланкою захисту будь-якої організації. Однак завдяки підвищенню обізнаності сучасним загрозам персонал може стати першою лінією кіберзахисту. Дізнатися більше про найпоширеніші онлайн-загрози та поради для захисту від них можна за посиланням.

Враховуючи вище перелічені виклики кібербезпеки, спеціалісти ESET нагадують про важливість дотримання основних правил, зокрема створення складних паролів, використання двофакторної автентифікації у всіх ваших акаунтах, здійснення онлайн-платежів лише на перевірених сайтах, а також забезпечення надійного захисту вашого смартфона, ноутбука та смарт-пристроїв». ***(10 викликів кібербезпеки: до чого готуватися користувачам та компаніям // AMC Ukraine (https://channel4it.com/publications/10-viklikv-kberbezpeki-do-chogo-gotuvatisya-koristuvacham-ta-kompanyam.html). 04.11.2022).***

***

«…Защита интеллектуальной собственности от хакеров имеет важное значение, поскольку в случае ее кражи бремя доказывания права собственности будет лежать на вас, если будет возбуждено судебное дело. В этой статье мы познакомим вас с некоторыми способами защиты интеллектуальной собственности от хакеров и обеспечения безопасности вашей работы.

Как обеспечить безопасность интеллектуальной собственности

Есть несколько способов защитить свою интеллектуальную собственность. В этом разделе мы рассмотрим некоторые из них:

Товарный знак и авторское право

В Великобритании вы получаете защиту авторских прав автоматически — вам не нужно подавать заявку или платить пошлину. У вас также есть возможность

пометить свою работу символом авторского права, вашим именем и годом создания. Однако то, делаете вы это или нет, не влияет на уровень вашей защиты. Авторское право может помешать людям копировать вашу работу, распространять или адаптировать ее без разрешения.

Вы также можете зарегистрировать свой товарный знак, чтобы защитить свой бренд. Это может включать название вашего продукта или услуги. Если вы решите зарегистрировать свой товарный знак, вы сможете подать в суд на любого, кто использует ваш бренд без разрешения, а также продает и лицензирует ваш бренд. Вы также сможете использовать символ зарегистрированного товарного знака, чтобы показать людям, что это ваш бренд, и удержать других от его использования.

В Великобритании товарный знак действует 10 лет, по истечении этого периода его необходимо продлить, чтобы он оставался в силе. Минимальная стоимость товарного знака составляет 170 фунтов стерлингов, но цена действительно зависит от ваших обстоятельств. С помощью товарного знака вы можете зарегистрировать следующее:

Логотипы

Звуки

Цвета

Слова

Товарный знак не только помогает защитить индивидуальность вашего бренда, но и устанавливает законное право собственности на вашу интеллектуальную собственность.

Будьте осторожны при использовании общественного Wi-Fi

В этом все более оцифрованном обществе мы обычно находимся всего в нескольких минутах ходьбы от общедоступной сети Wi-Fi. В большинстве общественных мест, от ресторанов до библиотек, есть бесплатный Wi-Fi.

Однако за эту свободу приходится платить, поскольку общедоступные сети Wi-Fi могут быть связаны с более высокими рисками безопасности. Таким образом, научившись защищать себя, вы обеспечите безопасность своей интеллектуальной собственности. Ниже приведены некоторые меры предосторожности при использовании общедоступного Wi-Fi:

При подключении к общедоступной сети Wi-Fi важно отключить общий доступ. Вы можете сделать это, отключив общий доступ в системных настройках или в разделе «Управление».

Панель

Всегда иметь актуальное решение для интернет-безопасности, установленное и работающее на вашем компьютере.

Использование подключения к виртуальной частной сети (VPN) является хорошей идеей при использовании бесплатного Wi-Fi. Это означает, что если бы вы оказались под угрозой кибератаки, ваши данные все равно были бы надежно зашифрованы.

Двухэтапная аутентификация

Когда дело доходит до защиты наших устройств и систем, слишком много людей вводят пароль, а затем называют его хорошим. Однако в современном мире

хакеры могут легко справиться с такой ненадежной защитой и похитить вашу интеллектуальную собственность до того, как вы поймете, что вас поразило.

В 2022 году имеет смысл добавить дополнительный уровень защиты вашей собственности с помощью двухэтапной аутентификации. Это акт требования двух отдельных факторов для доступа. Это может быть пароль и отпечаток большого пальца или пароль и код, отправленные текстовым сообщением на номер вашего мобильного телефона.

Также рекомендуется выработать привычку регулярно менять пароль и следить за тем, чтобы он был максимально непроницаемым (чтобы не было дней рождения, кличек домашних животных или других слов, которые можно легко угадать).

Аудит безопасности

Независимо от того, являетесь ли вы юридическим лицом или частным лицом, если вы владеете интеллектуальной собственностью, которая заслуживает защиты, вам необходимо выработать привычку проводить проверки безопасности на всех без исключения устройствах, которые вы и ваша компания используете. Это необходимо для того, чтобы ваши протоколы безопасности были настолько надежными, насколько это возможно для эффективной защиты от хакеров.

Обучайте сотрудников

Если ваша интеллектуальная собственность находится в системе, к которой имеют доступ сотрудники или другие люди, важно информировать людей о важности безопасности. И, в дополнение к этому, обучая их любым протоколам, которые вы установили.

Это особенно важно в 2022 году, когда больше сотрудников, чем когда-либо, работают удаленно. Всегда полезно установить правила для удаленных сотрудников, чтобы обеспечить безопасность; например, запрет на загрузку фильмов или других небезопасных материалов на их рабочие ноутбуки…» ***(Mic Johnson. How to Keep Your Intellectual Property Safe from Hackers // latesthackingnews.com (https://latesthackingnews.com/2022/11/21/how-to-keep-your-intellectual-property-safe-from-hackers/amp/). 21.11.2022).***

***

«Microsoft присоединилась к инициативе по обеспечению кибербезопасности Хартии доверия (CoT) с 10 ноября 2022 года. В качестве члена CoT Microsoft планирует поделиться своим опытом в области кибербезопасности для разработки и повышения осведомленности о надежных принципах безопасности для безопасного цифрового мира. С присоединением Microsoft инициатива Хартии доверия выросла до 18 участников. Siemens и восемь партнеров из промышленного сектора основали эту инициативу в 2018 году для продвижения достижений в области кибербезопасности в различных отраслях и на глобальном уровне.

«Хартия доверия воплощает в себе ценности, к которым мы в Microsoft относимся серьезно: быть активными, открытыми, прозрачными и сотрудничать в разработке передовых методов кибербезопасности и укреплении доверия», — говорит Том Берт, корпоративный вице-президент по безопасности клиентов и

доверию в Microsoft. «Отраслевое партнерство имеет решающее значение для решения проблем, с которыми мы сталкиваемся сегодня, и мы рассчитываем на сотрудничество с членами для продвижения стратегий и инициатив, укрепляющих кибербезопасность».

«Кибербезопасность — это ключ к укреплению доверия людей к цифровым технологиям, — говорит Седрик Нейке, член правления Siemens AG и генеральный директор Digital Industries. «Привлекая Microsoft, Хартия доверия снова приобретает значительно больший вес для того, чтобы сделать наш подключенный мир более устойчивым и сформировать наше цифровое будущее».

За последние четыре года Хартия доверия уже запустила множество мер по повышению кибербезопасности, включая принцип «Безопасность по умолчанию», который учитывает кибербезопасность прямо на этапе проектирования и предоставляет продукты с предварительно настроенными мерами безопасности. Кроме того, партнеры CoT определили базовые требования для своих поставщиков, чтобы еще больше повысить кибербезопасность во всех цепочках поставок. Основное внимание на следующем этапе будет уделено внедрению межотраслевого подхода к оценке безопасности цепочки поставок. В этом контексте растущее сообщество Charter of Trust будет предоставлять компаниям, в основном малым и средним предприятиям, информацию, обучение и дополнительные ресурсы.

Инициатива CoT регулярно сотрудничает с различными глобальными органами власти и научными учреждениями, чтобы также продвигать достижения в области кибербезопасности на международном уровне и согласовывать усилия за пределами национальных границ и организационных границ. С этой целью в рамках инициативы CoT был создан Форум ассоциированных партнеров, к которому присоединились такие учреждения, как Федеральное управление информационной безопасности Германии, Министерство внутренних дел и связи Японии (MIC), Канадский центр кибербезопасности и Xacco. Plattner Institute for Digital Engineering GmbH (HPI) в Германии.

На Мюнхенской конференции по безопасности в феврале 2018 года компания «Сименс» и восемь партнеров из промышленного сектора подписали первую в мире совместную хартию по повышению кибербезопасности. Помимо Siemens и Мюнхенской конференции по безопасности, в число подписантов входят AES, Airbus, Allianz, Atos, Bosch, Dell Technologies, Deutsche Post DHL Group, IBM, Infineon Technologies AG, Mitsubishi Heavy Industries, NTT, NXP Semiconductors, SGS, TotalEnergies, TÜV SÜD — а теперь и Microsoft». ***(Beatrice. Microsoft joins Charter of Trust for cyber security collaboration // All Things Media Ltd (https://dcnnmagazine.com/security/microsoft-joins-charter-of-trust/). 16.11.2022).***

***

«Ожидается, что к 2032 г. оценка рынка кибербезопасности превысит 900 млрд долларов США, как сообщается в исследовании, проведенном Global Market Insights Inc.

Растущая потребность в защите конфиденциальных персональных данных в секторе ИТ и телекоммуникаций привела к увеличению спроса на решения для кибербезопасности. Поскольку телекоммуникационные компании являются

ключевым компонентом инфраструктуры, поддерживающей функционирование связи, сектор телекоммуникаций стал основной мишенью киберрисков. Данные о клиентах — еще одна традиционная важная цель, связанная с отраслью. Кроме того, государственные органы обеспечивают соблюдение все большего числа правил соблюдения кибербезопасности. Чтобы защитить серверы, центры обработки данных и виртуальные информационные системы, предприятия внедряют решения для обеспечения безопасности, которые, как ожидается, дополнят рост рынка кибербезопасности.

Ограниченная осведомленность о решениях IAAM может помешать принятию продукта

Недостаток осведомленности организаций о многочисленных преимуществах систем управления идентификацией и доступом (IAAM) негативно сказывается на коммерческой статистике. Поскольку эти решения жизненно важны для защиты бизнеса от кибератак и предоставления доступа нужным пользователям к конфиденциальной информации, отсутствие надежной инфраструктуры кибербезопасности подвергает риску данные компании

Функция автоматического обновления системы для усиления потребности в едином управлении угрозами

Прогнозируется, что сегмент сетевой безопасности унифицированного управления угрозами (UTM) будет расти более чем на 20 % в год в период с 2023 по 2032 год. будущее.

Распространение интегрированных решений безопасности и IP-трафика для расширения доли рынка сетевой безопасности

Сегмент сетевой безопасности занимал около 15% доли рынка кибербезопасности в 2022 году, и ожидается, что к 2032 году будут наблюдаться значительные темпы роста. Компаниям сложно управлять сложными современными сетями по мере распространения новых сетевых архитектур. Таким образом, прогнозируется, что спрос на рынке решений для сетевой безопасности будет обусловлен увеличением IP-трафика и проникновением интегрированных решений безопасности.

Растущая склонность к цифровизации и автоматизации для стимулирования спроса на продукцию со стороны МСП

В зависимости от организации сегмент МСП должен показать рост почти на 15% в период с 2023 по 2032 год. Растущая склонность МСП к автоматизации, цифровизации, Интернету вещей и интеллектуальному производству привела к внедрению информационных технологий, преобразованию физических активов в цифровые активы и нулевая терпимость к нарушениям информационной безопасности. Все сообщения, транзакции и документы теперь оцифрованы и обмениваются онлайн. Тем не менее, это делает малые и средние предприятия главной мишенью для онлайн-злоумышленников и хакеров, что, как предполагается, увеличивает потребность в решениях для кибербезопасности в этих организациях.

Технологические достижения в транспортных средствах способствуют расширению транспортного сегмента

По оценкам, рынок кибербезопасности в сегменте конечных пользователей транспорта вырастет более чем на 10% до 2032 года благодаря растущему внедрению

IIoT, интеллектуальной логистики и цифровой инфраструктуры. Кроме того, для разработки новых технологий, таких как передовые технологии поддержки водителя в автономных транспортных средствах, требуется разнообразная электроника, датчики и компьютерные системы. Компании сосредоточены на создании надежной инфраструктуры кибербезопасности для борьбы с опасностями, поскольку они исследуют преимущества безопасности этих новых автомобильных технологий, которые предназначены для поддержки расширения сегмента.

Растущее использование интеллектуальных устройств для увеличения доходов рынка Латинской Америки

Ожидается, что к 2032 году рынок кибербезопасности в Латинской Америке превысит 100 миллиардов долларов США. Проблемы и уязвимости, связанные с кибербезопасностью, возросли в результате быстро меняющейся цифровой среды в регионе Латинской Америки. Растущее использование интеллектуальных устройств в сочетании с растущими государственными расходами на инфраструктуру широкополосной связи в значительной степени способствует увеличению доли региональных доходов…» ***(Cyber Security Market to Hit $900 Bn By 2032, Says Global Market Insights Inc. // Global Market Insights Inc. (https://www.globenewswire.com/news-release/2022/11/22/2560597/0/en/Cyber-Security-Market-to-Hit-900-Bn-By-2032-Says-Global-Market-Insights-Inc.html). 22.11.2022).***

***

«Гаагская программа по международной кибербезопасности фокусируется на различных способах управления, которые государства и другие субъекты могут использовать для решения и формирования стратегических задач в цифровой среде. Конференция этого года была посвящена международной кибербезопасности и роли новых технологий.

В этом году Гаагская программа по международной кибербезопасности организовала ежегодную научную конференцию и представила широкий обзор современных тем, связанных с кибербезопасностью. Среди участников было много ученых, экспертов и некоторых политиков из области международной кибербезопасности. Конференция проходила в отеле het Spaansche Hof, что создало потрясающую атмосферу для разговоров на тему кибербезопасности.

День 1: Современная область кибербезопасности

Приветствуя Денниса Бродерса, участники начали с того, что выслушали ключевого докладчика Джейсона Хили, который рассказал о силе и опасности кибернарративов для разработки политики. В перерывах между выступлениями ключевых спикеров и панельными дискуссиями участники могли пообщаться за вкусными блюдами. Одной из проблем, с которой столкнулись участники, был выбор следующей панельной дискуссии, поскольку все темы звучали очень интересно.

Сложность современных вопросов кибербезопасности стала очевидной во время всех переговоров, например, в отношении международного права и норм. Какими должны быть рассуждения государств о международных кибероперациях?

В одной из панельных дискуссий обсуждалась стратегическая игра на великих нарративах, что дало пищу для размышлений о стремлении к цифровому суверенитету в сложном глобальном киберрежиме. Еще одна дискуссия о национальных нарративах о кибербезопасности, была расшифрована китайская кибернарративность и представлено столкновение мнений Запада в китайско-индийском соперничестве. Также были затронуты война между Россией и Украиной и влияние СМИ на киберконфликт.

Первый день завершился выступлением Жозефины Вольф, в которой основное внимание было уделено эволюции рынка киберстрахования и его влиянию на кибербезопасность.

День 2: Киберопераци и дезинформация

Второй день начался с разговора об угрозах, инструментах и оружии со стороны России и Интернета. Киберпреступность также стала известна в ходе панельной дискуссии, посвященной поведению государства и использованию социальных сетей с точки зрения кибербезопасности.

Кроме того, с учетом правовых и нормативных вопросов, касающихся разведки, была представлена Теория справедливой разведки и подробно объяснено двойное использование в дискурсе шпионского ПО. Проблемы и возможности технологий и управления Интернетом были рассмотрены в перспективе, в то время как в другой панельной дискуссии говорилось о милитаризации кибер-разговоров.

Навигация по нарративам в киберпространстве

На финальном круглом столе обсуждались российские кибер-информационные операции в контексте войны на Украине. Возникли следующие вопросы: как Россия использует информационные операции, чтобы посеять раздор на западе в отношении Украины? Какие виды кибероперацiй мы видели в ходе конфликта? Изменилась ли тактика России с 2016 года? Какие дезинформационные нарративы преобладают? Есть ли у России последовательная информационная стратегия или операции носят реактивный характер? Как разные страны и платформы справились с этой проблемой?» ***(Successful Conference on International Cyber Security 2022 // Leiden University (https://www.universiteitleiden.nl/en/news/2022/11/successful-conference-on-international-cyber-security). 22.11.2022).***

***

Сполучені Штати Америки

«Крупные отраслевые группы спорили о том, как CISA должна определять ключевые термины в своем процессе нормотворчества для реализации федерального закона об отчетах об инцидентах.

Поставщики коммерческих информационных и коммуникационных технологий не должны быть обязаны сообщать об инцидентах кибербезопасности Агентству кибербезопасности и безопасности инфраструктуры, сообщила торговая ассоциация некоторых из крупнейших таких компаний агентству, которое

возглавляет процесс разработки правил для реализации закона об отчетах об инцидентах. для критической инфраструктуры.

В комментариях Совета индустрии информационных технологий, опубликованных во вторник в пресс-релизе, группа, в которую входят такие компании, как Microsoft, CISCO и Zoom, заявила, что «обзор должен соответствовать национальной оценке критичности».

«Такой подход следует поощрять, чтобы сузить круг, когда организации действительно выполняют критически важные для страны функции, имеющие значение для национальной безопасности, такие как спутниковая связь, по сравнению с коммерческими вариантами использования», — пишут компании. «Если система не имеет разумной привязки к важнейшей функции на национальном уровне, ее не следует охватывать».

В марте Конгресс принял Закон об отчетах о кибер-инцидентах для критически важной инфраструктуры в ответ на то, что обычно называют взломом SolarWinds. Хакеры смогли получить доступ к активам, принадлежащим поставщику готовых коммерческих ИТ, а также Microsoft, в ходе кампании, которая в конечном итоге скомпрометировала девять федеральных агентств и по меньшей мере сотню американских компаний. Взломы не были обнаружены до тех пор, пока они не были добровольно раскрыты фирмой по кибербезопасности FireEye, которая была среди скомпрометированных.

Законодатели, продвигающие законодательство, рассмотрели необходимость требовать отчетов об инцидентах кибербезопасности, чтобы предупредить других в подключенной экосистеме и смягчить эффект каскадного воздействия на экономику на фоне роста числа программ-вымогателей и других кибератак. Но Конгресс оставил на усмотрение CISA решение о том, какие организации должны подпадать под действие закона и о каких инцидентах следует сообщать.

«Владельцы и операторы критической инфраструктуры должны полагаться на своих поставщиков технологий и поставщиков услуг и доверять им», — написали технологические компании, ссылаясь на формулировку закона. «Таким образом, третьи стороны/сторонние поставщики должны быть исключены из сферы охвата юридических лиц. Отчетность должна падать только на сам пострадавший объект».

Торговые ассоциации финансового сектора не согласились. В пресс-релизе со своими собственными комментариями для CISA во вторник Американская ассоциация банкиров, Институт банковской политики и другие заявили, что «требование о предоставлении отчетности должно применяться в равной степени к критическим и некритическим услугам».

«Многие поставщики технологий, такие как облачные сервисы и агрегаторы данных, имеют доступ к большим объемам конфиденциальных данных», — пишут группы финансового сектора. «Требование отчетности только от критически важных секторов инфраструктуры игнорирует существенность инцидента и возможные системные риски».

В комментариях финансового сектора также содержится призыв к более высокому порогу для запроса отчетов об инцидентах, несмотря на то, что один из его собственных руководителей — директор по безопасности Mastercard Рон Грин — недавно выступил за более низкий порог отчетности, отметив, что это приведет к

большему успеху в соответствии с духом закон. На мероприятии, организованном Центром стратегических и международных исследований, директор по стратегии CISA Валери Кофилд также подчеркнула преимущества агентства, использующего более низкий порог для стимулирования отчетности.

«Критерии сообщения должны основываться на обстоятельствах и серьезности инцидента. Только о серьезных и угрожающих инцидентах (т. е. со злым умыслом) следует сообщать», — заявили в банковской группе. «От организаций не следует требовать сообщать о технологических сбоях или других прерываниях, связанных с обслуживанием, которые, хотя и неудобны, но не представляют системных угроз».

В комментариях ITI также говорится, что CISA должна «ограничить отчетность серьезными и значительными атаками, которые вызывают фактические сбои или потери, и включать определенные параметры», среди прочих критериев.

Общественные комментарии по нормотворческим усилиям CISA должны были появиться в понедельник». ***(Mariam Baksh. Big Tech Tells CISA to Exempt Third-Party Providers from Incident Reporting Rule // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/big-tech-tells-cisa-exempt-third-party-providers-incident-reporting-rule/379830/). 17.11.2022).***

***

«Счетная палата правительства обнаружила, что Пентагону «не хватает подотчетной организации и последовательного руководства» для документирования и обмена подробностями о зарегистрированных киберинцидентах.

Хотя министерство обороны в последние годы предприняло шаги для успешного смягчения угроз кибербезопасности для военных информационных систем, оно должно лучше управлять и полностью внедрять свои процессы обмена инцидентами, согласно отчету, опубликованному Счетной палатой правительства в понедельник.

Конгресс потребовал, чтобы GAO провело оценку «усилий Министерства обороны по управлению кибер-инцидентами» в отчете Палаты представителей, который сопровождал Закон о разрешении на национальную оборону на 2021 финансовый год.

В рамках обязательной проверки, которая проводилась с марта 2021 года по ноябрь 2022 года, были опрошены 24 поставщика услуг кибербезопасности, или CSSP, которые «предоставляют услуги кибербезопасности компонентам Министерства обороны США». Затем GAO проанализировало кибер-инциденты, выявленные CSSP в своих сетях с 2015 по 2021 год, и были включены в Совместную систему управления инцидентами Министерства обороны США, или JIMS, которая служит официальным хранилищем задокументированных кибер-инцидентов Министерства обороны США.

«Согласно данным JIMS, CSSP Министерства обороны сообщили о 12 077 кибер-инцидентах, затрагивающих их сети с 2015 по 2021 календарный год», — говорится в отчете. «За этот период количество инцидентов, о которых сообщили CSSP, снизилось с 3880 в 2015 году до 948 в 2021 году».

GAO объяснило сокращение зарегистрированных кибер-инцидентов «увеличением развертывания механизмов защиты департамента в течение этого периода времени», отметив, что Министерство обороны установило два процесса — «один для всех инцидентов и один для критических инцидентов» — чтобы упростить отчетность. и управленческие усилия. Однако, несмотря на уменьшение зарегистрированных кибер-инцидентов, GAO обнаружило, что Министерство обороны «не полностью внедрило ни один из процессов» и что в департаменте «не хватает подотчетной организации и последовательного руководства для обеспечения полной и обновленной отчетности обо всех кибер-инцидентах».

Проверка GAO показала, что 91% отчетов о кибер-инцидентах JIMS, представленных в течение анализируемого периода времени, «не включали информацию о дате обнаружения инцидента, что препятствовало способности Министерства обороны определять, были ли сообщения об инцидентах своевременными в JIMS». Еще 68% отчетов «не включали информацию о векторе доставки инцидента, что ограничивало способность Министерства обороны выявлять тенденции распространенности различных угроз, затрагивающих его сети».

«Помимо неполной информации об инцидентах, CSSP также не всегда уведомляли руководство Министерства обороны США об инцидентах, которые оказали негативное влияние на способность Министерства обороны выполнять свою миссию или доступность его сетей», — говорится в отчете. «В частности, у CSSP не было доказательств того, что они уведомили соответствующее руководство примерно о 47 процентах инцидентов, о которых они сообщили в календарных годах с 2015 по 2020».

GAO также обнаружило, что Министерство обороны «еще не решило», следует ли сообщать об обнаруженных киберинцидентах, затрагивающих базу оборонной промышленности страны, которая, как говорится в отчете, «включает в себя организации, не входящие в федеральное правительство, которые предоставляют товары или услуги, имеющие решающее значение для удовлетворения военных требований США». со всеми соответствующими заинтересованными сторонами».

«В руководстве Министерства обороны говорится, что для защиты интересов национальной безопасности киберинциденты должны координироваться между организациями Министерства обороны и внешними источниками, такими как партнеры [базы оборонной промышленности]», — говорится в отчете. «Пока Министерство обороны не рассмотрит, следует ли делиться этой информацией со всеми соответствующими сторонами, могут быть упущены возможности для выявления системных угроз и устранения слабых мест системы».

GAO также обнаружило, что сообщения об утечках данных, связанных с информацией, позволяющей установить личность, или PII, «увеличились на 104 процента с 2015 по 2021 календарный год». Хотя в отчете отмечается, что Министерство обороны «установило процесс для определения того, следует ли уведомлять лиц о нарушении их личной информации», в нем было обнаружено, что министерство также «не последовательно документировало оценки рисков или уведомления затронутых лиц».

«Без документирования уведомления невозможно проверить, действительно ли Министерство обороны информировало людей о том, что их конфиденциальные данные были потенциально скомпрометированы, что может сделать некоторых затронутых лиц более уязвимыми для кражи личных данных, чем другие», — отмечается в отчете.

GAO дало Министерству обороны шесть рекомендаций, в том числе о том, что департамент «возлагает ответственность за обеспечение надлежащей отчетности об инцидентах, улучшает обмен информацией о кибер-инцидентах, связанной с DIB, и документирует, когда затронутые лица уведомляются о нарушении PII». Министерство обороны согласилось со всеми шестью рекомендациями GAO». ***(Edward Graham. DOD Must Enhance Cyber Incident Reporting and Sharing, Watchdog Says // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/dod-must-enhance-cyber-incident-reporting-and-sharing-watchdog-says/379776/). 16.11.2022).***

***

«В ходе 120-дневного спринта в рамках инициативы было нанято более 7000 учеников.

Администрация Байдена завершила 120-дневный спринт по кибербезопасности во вторник — во время Национальной недели ученичества — в рамках постоянных усилий по удовлетворению потребностей в рабочей силе.

Президент Джо Байден организовал спринт, чтобы помочь удовлетворить растущие потребности страны в кибербезопасности, стремясь создать разнообразную, надежную и квалифицированную рабочую силу. Программа направлена на то, чтобы работодатели, отраслевые ассоциации, профсоюзы и поставщики услуг по обучению взаимодействовали с системой зарегистрированного ученичества, в которой программы ученичества проверяются промышленностью и утверждаются Министерством труда или государственным агентством, в качестве стратегии найма, обучения и удержание путем создания новой программы ученичества или присоединения к существующей.

В результате этой программы были утверждены или находятся в стадии разработки 194 новые программы зарегистрированного обучения в области кибербезопасности. Кроме того, новые и существующие спонсоры программ расширили свои программы, добавив 120 профессий, связанных с кибербезопасностью, к существующим и новым программам зарегистрированного обучения. Крупные организации, такие как IBM, Cisco Systems, Power, CompTIA и Министерство обороны, создали новые или расширили существующие программы зарегистрированного обучения.

Например, программа военного ученичества United Services Министерства обороны спонсирует крупнейшую программу зарегистрированного ученичества в области кибербезопасности. В рамках USMAP в январе 2022 года Министерство обороны США и Министерство обороны создали первую федеральную программу обучения кибербезопасности. В рамках программы Министерство обороны США определило и установило стандарты для 15 профессий, связанных с критической инфраструктурой кибербезопасности. С тех пор все стандарты были одобрены, и 10 были утверждены во время спринта. Министерство обороны также выпустило

меморандум, поощряющий использование программ ученичества для расширения штата специалистов по кибербезопасности.

Тем временем Департамент по делам ветеранов в рамках спринта учредил первую федеральную программу обучения кибербезопасности для гражданских лиц. Программа призвана стать образцом для найма ветеранов на работу в сфере кибербезопасности, и первая группа из 8-10 учеников начнет работу в феврале 2023 года.

«Завершение Национального спринта по обучению кибербезопасности — важная веха, частью которой мы гордимся, но работа по развитию кибер-талантов продолжается», — сказала Эми Кардел, старший вице-президент по взаимоотношениям с персоналом в ассоциации ИТ-индустрии CompTIA. «Каждый день нам напоминают о киберугрозах, с которыми мы сталкиваемся как отдельные лица, как организации и как нация. Самая надежная защита начинается с высококвалифицированного и сертифицированного персонала в области кибербезопасности».

В рамках этой инициативы было нанято более 7000 учеников, большинство из которых были наняты по программам, не связанным с частным сектором. Из более чем 1000 учеников в частном секторе 42% — цветные люди, а 32% — женщины. До этой инициативы 27% учеников по кибербезопасности были цветными, а 28% — женщинами, что, согласно объявлению, «отражает влияние этого спринта и силу совместной работы государственного и частного секторов и партнерства с общественными организациями». организаций для охвата различных слоев населения».

Кроме того, более 2000 организаций и людей, ищущих работу, выразили заинтересованность в получении информации о зарегистрированном обучении.

Спринт кибер-ученичества проводился Министерством труда при содействии Белого дома, офиса Национального кибер-директора, а также Министерства торговли, Министерства внутренней безопасности и Министерства обороны, а также других агентств.

«120-дневный спринт по обучению кибербезопасности повысит осведомленность о текущих успешных программах зарегистрированного обучения, связанных с кибербезопасностью, а также привлечет работодателей и отраслевые ассоциации для расширения и продвижения зарегистрированного обучения как средства предоставления работникам высококачественных, зарабатывающих по мере обучения обучение для хорошо оплачиваемой работы в области кибербезопасности», — сказал министр труда Марти Уолш. «Эти недавно обученные работники помогут защитить нашу критически важную инфраструктуру, улучшить наш цифровой образ жизни, укрепить нашу экономику и улучшить доступ к карьерным возможностям в области кибербезопасности для недостаточно представленных сообществ, особенно женщин, цветных людей, ветеранов и людей с ограниченными возможностями». ***(Kirsten Errick. White House Sprint Ends With Nearly 200 New Cyber Apprenticeship Programs // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/white-house-sprint-ends-nearly-200-new-cyber-apprenticeship-programs/379773/). 16.11.2022).***

***

«Администрация Байдена обращается к Конгрессу за помощью в «восполнении пробелов в законных полномочиях» для улучшения кибербезопасности США.

Секретарь Министерства внутренней безопасности Алехандро Майоркас предложил, чтобы политика США в области кибербезопасности по-прежнему полагалась на поставщиков критически важных услуг, добровольно применяющих меры для защиты своих операций от кибератак.

Во вторник Майоркас вместе с директором ФБР Кристофером Рэем дал показания перед Комитетом по внутренней безопасности Палаты представителей о глобальных угрозах родине. Кибербезопасность составляет все более значительную часть ежегодных слушаний, которые в этом году были сосредоточены на множестве национальных государств и криминальных противников.

Обращаясь ко всем свидетелям, уходящий в отставку член палаты представителей Джим Ланжевин, доктор медицинских наук, спросил: «Какие пробелы мы должны заполнить, связанные с повышением кибербезопасности критической инфраструктуры?»

Ланжевен поставил свой вопрос в контексте письма президента Джо Байдена от 7 ноября, которое он написал избранным комитетам Конгресса, в котором отмечалось: «Нашей стране не хватает всеобъемлющего способа установить обязательные минимальные требования к кибербезопасности для нашей критически важной инфраструктуры, и текущие подходы различаются в зависимости от сектора.»

«Моя администрация надеется на сотрудничество с Конгрессом, чтобы заполнить пробелы в законных полномочиях, чтобы обеспечить защиту нашей критически важной инфраструктуры от кибератак», — говорится в письме.

Майоркас не ответил прямо на вопрос. Вместо этого он рассказал о действиях, уже предпринятых Управлением транспорта и безопасности DHS и Агентством кибербезопасности и безопасности инфраструктуры. В случае с CISA он высоко оценил опубликование добровольных целей в области кибербезопасности и сказал, что агентству следует сосредоточить свои усилия на международном сотрудничестве.

Рэй также не ответил прямо на вопрос, но дал оценку отношениям ФБР с фирмами, занимающимися кибербезопасностью, и заинтересованными сторонами в критически важной инфраструктуре после усилий по смягчению последствий российских кибератак против Украины.

«Партнерство с частным сектором является важнейшим элементом защиты критической инфраструктуры в этой стране», — сказал он. «И я думаю, что мы добились очень значительного прогресса. Предстоит еще много работы, но, на мой взгляд, мы на правильном пути».

Рэй подчеркнул важность роли отрасли в обеспечении безопасности критической инфраструктуры, более 80% которой находится под частным контролем, подчеркнув потенциальное изменение целей противника.

«Это становится все более и более переполненным полем действий злоумышленников, нацеленных на критически важную инфраструктуру», — сказал

он, добавив. «Одна из вещей, которая нас особенно беспокоила во время российско-украинского конфликта, — это возможность того, что, например, российские спецслужбы, которые давно нацелены на нашу критическую инфраструктуру в шпионских целях, могут использовать тот же доступ для более разрушительных целей. целей». ***(Mariam Baksh. DHS Chief Appears to Back Status Quo Approach for Securing Critical Infrastructure // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/dhs-chief-appears-back-status-quo-approach-securing-critical-infrastructure/379763/). 15.11.2022).***

***

«В отчете комиссии также содержится призыв к администрации Байдена рассмотреть вопрос об отмене статуса Китая в качестве привилегированного торгового партнера, если проверка Конгресса обнаружит, что Пекин не выполняет свои обязательства.

Согласно отчету, опубликованному во вторник консультативной комиссией Конгресса, внимание Китая к расширению своих кибервозможностей за последнее десятилетие «представляет огромную угрозу для Соединенных Штатов в киберпространстве сегодня». Это предупреждение дополняет оценку комиссии о том, что торговая практика Пекина требует более пристального внимания со стороны законодателей и администрации Байдена.

В годовом отчете Американо-китайской комиссии по обзору экономики и безопасности за 2022 год для Конгресса оценивается ряд угроз для экономики и национальной безопасности США, включая кибервойну Пекина и возможности шпионажа. Комиссия, созданная Конгрессом в 2000 году и включающая 12 членов, назначенных лидерами демократов и республиканцев в Палате представителей и Сенате, должна ежегодно отчитываться о «последствиях экономических отношений между Соединенными Штатами и Китайской Народной Республикой для национальной безопасности».

В отчете комиссии отмечается, что стремление Пекина стать «кибер-сверхдержавой» дает Китаю «асимметричное преимущество перед Соединенными Штатами в киберпространстве из-за нежелания [Коммунистической партии Китая] играть по тем же правилам, что отражает динамику, наблюдаемую в других областях. Отношения США и Китая». А растущая зависимость Пекина от кибероперaций — для проведения информационных войн, проведения кибершпионажа и продвижения своих интересов национальной безопасности путем контроля над киберпространством — «представляет серьезную угрозу для правительства США, бизнеса и критически важных инфраструктурных сетей в новом и высококонкурентном киберпространстве».

«Страна добилась этой трансформации за счет реорганизации своих институтов, определяющих киберполитику, разработки сложных наступательных кибер-возможностей и осуществления кибершпионажа с целью кражи иностранной интеллектуальной собственности в промышленных масштабах», — говорится в отчете.

В частности, операции Пекина по кибершпионажу, которые, согласно отчету, «становятся все более изощренными и используют передовые тактики», часто

полагаются на «эксплуатацию уязвимостей и компрометацию третьих сторон для проникновения в сети жертв». И эти усилия дополнительно подкрепляются тем фактом, что законодательство Китая, связанное с кибербезопасностью, «предоставляет оружие индустрии и исследованиям в области кибербезопасности в стране, требуя от компаний и исследователей представлять правительству все обнаруженные уязвимости в программном и аппаратном обеспечении, прежде чем предоставлять их поставщикам, которые могут их исправить».

Чтобы лучше бороться с операциями Китая в киберпространстве, комиссия рекомендовала Конгрессу принять закон о кодификации «системно важной критичной инфраструктуры», а также потребовать от определенных «организаций, оборонных подрядчиков и получателей федерального финансирования исследований и разработок чувствительных и новых технологий проводить усиленную защиту» и меры по смягчению последствий кибератак».

В отчете также рекомендуется, чтобы Конгресс поручил Министерству внутренней безопасности «каталогизировать китайское оборудование для наблюдения, системы экстренного реагирования и системы умных городов, используемые правительствами штатов и местными органами власти», и реализовать планы по «удалению и замене такого оборудования для защиты интересов США».

В отчете, опубликованном Центром безопасности и новых технологий Джорджтаунского университета в прошлом месяце, говорится, что по крайней мере 1681 правительств и местные органы власти в 49 штатах приобрели информационные и коммуникационные технологии и услуги у пяти китайских компаний, которые были запрещены федеральным правительством в период с 2015 по 2021 год.

Кроме того, комиссия рекомендовала Управлению торгового представителя США составить обновляемый список китайских компаний в критически важных секторах, «которые, как было установлено, извлекли выгоду из принудительной передачи интеллектуальной собственности», который можно использовать для запрета инвестиций в компании и отказа в экспортных лицензиях для фирмы. В отчете также содержится призыв к Конгрессу потребовать от министерства финансов запретить инвестиции в китайские фирмы, занимающиеся «сбором разведывательных данных с использованием кибертехнологий или кражей интеллектуальной собственности, спонсируемой Китайской Народной Республикой, против лиц, проживающих в США».

«Остаются срочные вопросы, касающиеся готовности Соединенных Штатов к кибератаке Китая, включая достаточность ресурсов для военных киберсил США, достаточность существующих средств защиты критической инфраструктуры США и масштабы сотрудничества между государственным и частным секторами в области кибербезопасности», — говорится в отчете.

Четыре из 39 рекомендаций отчета для Конгресса касались кибервозможностей Китая, в то время как другие в основном касались проблем, связанных с Гонконгом, Тайванем, экономикой США и национальной безопасностью. Однако главная рекомендация комиссии заключалась в том, чтобы Конгресс поручил администрации Байдена провести обзор постоянных нормальных торговых отношений Пекина — или PNTR — статуса, утвержденного Конгрессом в

2000 году, когда Китай готовился присоединиться к Всемирной торговой организации.

Кимберли Глас, президент и главный исполнительный директор Национального совета текстильных организаций и заместитель председателя комиссии, заявила во вторник во время публичного брифинга по поводу доклада, что, когда был утвержден статус Китая в PNTR для нормализации торговых отношений с Пекином, «было признание того, что условия, на которые согласился Китай, — если он их выполнит — устранили бы системные искажения в торговле, с которыми сталкиваются американские компании и рабочие, и уравняли бы игровое поле».

Но принудительная передача технологий, кража американской интеллектуальной собственности и ограничения доступа к рынку вызвали обеспокоенность по поводу сохранения Пекином статуса PNTR. Глас сказал, что участие Китая в этой деятельности «нанесло ущерб экономике США, работникам и нашим цепочкам поставок, создав значительные уязвимые места для экономической и национальной безопасности Соединенных Штатов».

В отчете Конгрессу рекомендуется поручить администрации Байдена подготовить отчет «в течение 90 дней» о соблюдении или несоблюдении Китаем двустороннего американо-китайского соглашения 1999 года о доступе на рынок. Если выяснится, что Пекин не соблюдает соглашение, в отчете говорится, что Конгресс «должен рассмотреть закон о немедленной приостановке постоянного режима нормальных торговых отношений Китая». Отзыв Пекином статуса PNTR может привести к тому, что США введут значительно более высокие тарифы на китайский импорт.

Публикация доклада комиссии состоялась после того, как президент Джо Байден и председатель КНР Си Цзиньпин провели трехчасовую встречу на полях саммита G20 в Индонезии в понедельник, чтобы обсудить ряд американо-китайских вопросов, включая провокации Северной Кореи и все более активную политику Пекина. милитаристская позиция по отношению к Тайваню». ***(Edward Graham. China's Cyber Capabilities 'Pose a Serious Threat' to US, Advisory Panel Warns // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/chinas-cyber-capabilities-pose-serious-threat-us-advisory-panel-warns/379760/). 15.11.2022).***

***

«Выполнение федеральными агентствами руководящих принципов NIST по этому вопросу — под руководством Конгресса — совпадает с сопротивлением отрасли комплексному подходу, который, по мнению заинтересованных сторон, необходим.

Поскольку федеральные агентства приближаются к крайнему сроку, установленному Конгрессом для контроля закупок устройств, способных подключаться к Интернету, ключевой чиновник из Национального института стандартов и технологий подчеркнул роль облачных сервисов и других поставщиков инфраструктуры, помимо производителей устройств, в смягчении последствий кибератак. которые стремятся использовать свои связи.

«Продукт часто представляет собой нечто большее, чем просто то, что [клиенты] установили», — говорит Катерина Мегас, руководитель программы NIST по кибербезопасности для Интернета вещей. «Часто есть мобильное приложение, которое контролирует доступ к устройству, [которое] позволяет вам получить доступ к данным на устройстве; это может позволить вам включать и выключать его. Часто это устройство подключено к облаку».

Мегас говорил во вторник на мероприятии, организованном Американским институтом предпринимательства. Она руководила подготовкой NIST серии документов, которые в совокупности образуют руководящие органы, которым должны следовать Закон об улучшении кибербезопасности IoT, двухпартийный законопроект, одобренный Конгрессом в конце 2020 года и получивший высокую оценку со стороны должностных лиц по кибербезопасности.

Среди документов есть каталог возможностей устройств, которые агентства могут использовать для информирования о своих новых требованиях к закупкам, которые, как отмечает Megas, должны быть активированы в декабре в соответствии с законом. Агентства могут рассмотреть вопрос о том, чтобы поставщики разрешали им изменять пароли, необходимые для доступа к их устройствам, например, в соответствии с каталогом.

В связи с Законом об улучшении кибербезопасности IoT NIST также ссылается на набор документов — серию 8259 — которые появились в результате исполнительного распоряжения администрации президента Дональда Трампа. Этот приказ от мая 2017 года был направлен на создание «устойчивости к ботнетам и другим автоматизированным распределенным угрозам». Результатом стала дорожная карта, в которой были определены роли и обязанности не только производителя устройств, но и конечных пользователей устройств на предприятиях, а также поставщиков интернет-услуг, которые предоставляют инфраструктуру, соединяющую их друг с другом.

«Мы должны быть уверены, что не упускаем из виду тот факт, что все взаимосвязано», — сказал Мегас. «Мы всегда предупреждали: «Давайте не будем просто говорить, что ответственность за кибербезопасность лежит [только] на производителях устройств». Это действительно экосистема. Вы не можете просто ожидать, что устройство будет безопасным, потому что оно очень взаимосвязано».

Дорожная карта 2018 года была поддержана основными заинтересованными сторонами в отрасли, в том числе телекоммуникационной отраслью, которые согласились с важностью мер по обеспечению безопасности систем интернет-маршрутизации, таких как протокол пограничного шлюза, для защиты от атак ботнетов, когда хакеры могут вызвать широкомасштабное опровержение услуги по сети, дистанционно управляя угнанными IoT-устройствами.

Но поскольку другие федеральные агентства призывают Федеральную комиссию по связи рассмотреть возможность выхода за рамки добровольных инициатив для отрасли по устранению уязвимостей в системе маршрутизации, отрасль выступает против такого регулирования.

«Уважайте процесс разработки стандартов Интернета с участием многих заинтересованных сторон», — говорится в отчете от 2 ноября Технической консультативной группы по широкополосному Интернету, некоммерческой

организации, спонсируемой поставщиками интернет-услуг, такими как Comcast и AT&T. «Если рассматривается регулирование, ставьте цели, а не конкретизируйте технологии».

На сцене с Megas во время мероприятия AEI Брайан Скрибер, вице-президент по технологиям безопасности и конфиденциальности CableLabs — торговой ассоциации кабельной промышленности, которая поставляет такие устройства, как кабельные коробки, модемы и маршрутизаторы, также высказал несогласие с аспектом NIST. руководящие принципы для закупок агентствами IoT.

Самая первая возможность устройства, указанная в каталоге потенциальных требований NIST, — это способность устройства идентифицировать себя. NIST увидел полезность производителей устройств, включающих так называемое описание использования производителя — или MUD — файл в свои продукты в связи с проектом агентства под названием «сигнализация о намерениях устройства».

«Устройство может отправить сообщение маршрутизаторам и сказать: «Я лампочка… Я не должен разговаривать с термостатом в моем доме». Эта лампочка не должна разговаривать с другими вещами», — сказал Мегас, описывая проект.

Ссылаясь на обязанности корпоративных клиентов, таких как агентства, Скрибер сказал: «[MUD] возлагает на кого-то странное бремя решения проблемы ниже по течению», добавив, что «нет экономического стимула возвращаться и обязательно обновлять это устройство».

Мегас защищал включение MUD в руководство NIST, ссылаясь на аналогичный документ, подготовленный агентством, в котором описываются обязанности клиентов в области IoT в связи с указом президента Джо Байдена о кибербезопасности. Она подчеркнула, что заинтересованные стороны должны принять концепцию «глубокоэшелонированной защиты» для эффективного повышения кибербезопасности Интернета вещей с помощью комплексного подхода». ***(Mariam Baksh. NIST Official Warns Against Device-only Approach to Securing IoT // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/nist-official-warns-against-device-only-approach-securing-iot/379595/). 10.11.2022).***

***

«Несмотря на «несколько» DDoS-атак, направленных на сайты государственных и местных выборов, а также на некоторые технические сбои, затрагивающие оборудование для голосования, CISA заявляет, что не обнаружила «активности», которая должна подорвать веру в результаты промежуточных выборов.

Несмотря на то, что во время промежуточных выборов 2022 года было несколько отдельных кибератак, направленных на веб-сайты государственных и местных выборов, высокопоставленный сотрудник Агентства кибербезопасности и безопасности инфраструктуры сообщил журналистам во время серии телеконференций во вторник, что они не наблюдали «конкретной или реальной угрозы нарушения избирательной инфраструктуры». или операций в день выборов».

«Мы не видели никаких действий, которые могли бы заставить кого-либо усомниться в безопасности, целостности или устойчивости нашей избирательной инфраструктуры», — добавил высокопоставленный представитель CISA.

В преддверии недавних промежуточных выборов CISA тесно сотрудничала с государственными и местными юрисдикциями, чтобы помочь должностным лицам успешно выявлять и предотвращать киберугрозы, а также лучше реагировать на угрозы насилия в отношении должностных лиц на выборах. 14 штатов также задействовали свои группы кибербезопасности Национальной гвардии, чтобы помочь защитить системы, связанные с голосованием, от цифрового вторжения.

Эти усилия по кибербезопасности оказались в значительной степени успешными на этих выборах, поскольку CISA заявила, что она «проверила лишь несколько» юрисдикций, которые, как сообщается, испытали распределенные атаки типа «отказ в обслуживании» или DDoS-атаки, которые пытаются нарушить доступ к веб-сайтам и серверам, подавляя их. манипулировали онлайн-трафиком, часто с помощью ботов или сети захваченных компьютеров.

В Миссисипи веб-сайт госсекретаря, который служит цифровым ресурсом для информации, связанной с выборами, и не участвует в подсчете голосов, был временно недоступен после «аномально большого увеличения объема трафика из-за DDoS-активности», говорится в сообщении офиса.

«Мы хотим быть предельно ясными и заверить жителей Миссисипи, что наша избирательная система безопасна и не была скомпрометирована», — добавила канцелярия госсекретаря.

Российская хакерская группа, которая ранее объявила о своем намерении атаковать политические веб-сайты в день выборов, взяла на себя ответственность за атаку в сообщении Telegram, хотя высокопоставленный представитель CISA сказал, что «мы не видели никаких доказательств того, что они являются частью широкомасштабная скоординированная кампания».

Ранее в тот же день офис клерка округа Шампейн в Иллинойсе также сообщил о проблемах с подключением и сбоях в работе, которые, по его словам, в сообщении Facebook, вероятно, были вызваны «кибератаками в сети и серверах».

Однако CISA заявила, что эти ограниченные кибератаки не повлияли на избирательный процесс.

«Важно помнить, что даже успешная DDoS-атака не влияет на способность пользователя проголосовать или подсчитать его», — сказал высокопоставленный представитель CISA, отметив, что большинство пострадавших веб-сайтов, о которых ему было известно, были быстро восстановлены.

В преддверии промежуточных выборов федеральные чиновники и исследователи в области безопасности также выразили обеспокоенность по поводу влияния дезинформации на избирательный процесс. В отчете, опубликованном в понедельник компанией Insikt Group, занимающейся кибербезопасностью, говорится, что ложные сведения о машинах для голосования, многие из которых распространились в социальных сетях после президентских выборов 2020 года, вновь появлялись в дни, предшествовавшие промежуточным выборам, и были может увеличиться после выборов.

В то время как в некоторых юрисдикциях в день выборов возникли относительно незначительные технические проблемы с их машинами и системами для голосования, некоторые отрицатели выборов и сторонники теории заговора

поспешили выделить проблемы как необоснованные примеры предвыборных махинаций.

В округе Марикопа, штат Аризона, самом густонаселенном округе штата, официальные лица сообщили, что машины для подсчета голосов в 60 избирательных участках не могли принимать заполненные бюллетени из-за неисправности печати. Должностные лица окружных избирательных комиссий заявили, что сбой не приводил к тому, что табуляторы для голосования неправильно считывали бюллетени, и что они использовали «безопасную урну для голосования» для хранения заполненных бюллетеней, пока были внесены необходимые исправления.

Учитывая статус Аризоны как ключевого штата на поле битвы в среднесрочной перспективе, а ключевые сенатские и губернаторские гонки еще не решены, некоторые республиканские законодатели и правые деятели ухватились за проблему, чтобы распространять необоснованные заявления о мошенничестве и дезинформацию о длительном времени ожидания для голосования в ключевом округе. Однако высокопоставленный чиновник CISA заявил, что «нет никаких доказательств злонамеренной деятельности или каких-либо злоупотреблений», и добавил, что «это техническая проблема, и они решили ее».

«Когда у вас есть 8 800 отдельных избирательных округов, вы увидите, что возникнет несколько проблем», — добавил представитель CISA. «Мы видели несколько таких сегодня, как это происходит в каждый день выборов. В этом нет ничего необычного, и очень важно, чтобы мы все работали над тем, чтобы нормальное не превратилось в гнусное». ***(Edward Graham. No 'Specific or Credible' Cyber Threats Affected Integrity of Midterms, CISA Says // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/no-specific-or-credible-cyber-threats-affected-integrity-midterms-cisa-says/379546/). 09.11.2022).***

***

«На следующий день после промежуточных выборов во вторник ни одна политическая партия еще не может претендовать на контроль над любой из ветвей Конгресса. В нынешнем виде Палата представителей склоняется к республиканцам, Сенат — к демократам, и могут пройти дни или недели, прежде чем уляжется предвыборная пыль.

Хотя «красная волна», которую предсказывали многие, не осуществилась, смена контроля, по крайней мере, в Палате представителей кажется вероятной, а изменения в одной или обеих палатах будут иметь серьезные последствия для федеральной кибербезопасности, технической политики и того, как администрация Байдена управляет.

«Если мы увидим раскол в Конгрессе, то, вероятно, на Холме возникнет еще больший тупик, и если Конгресс полностью контролируется одной партией, а президент — другой, можно только представить, как в нынешней политической обстановке будут бодаться головой. — заявил Nextgov Стэн Солоуэй, президент и главный исполнительный директор Celero Strategies и бывший сотрудник отдела закупок министерства обороны. «Если обе палаты уйдут, сделать что-либо станет кошмаром».

Солоуэй сказал, что раскол Конгресса, вероятно, препятствует принятию какого-либо важного технологического законодательства, такого как всеобъемлющий закон о конфиденциальности. Климатическое законодательство также будет заблокировано. Тем не менее, Солоуэй сказал, что федеральная ИТ-модернизация «остается беспристрастной» — это одна из немногих областей соглашения для обеих сторон — наряду с желанием улучшить предоставление государственных услуг. Это может быть хорошей новостью для федеральных ИТ-бюджетов, которые увеличились за последние пять лет при президентах и конгрессах республиканцев и демократов.

Однако Солоуэй предупредил, что палата представителей, возглавляемая республиканцами и имеющая право выделять средства, скорее всего, пересмотрит и изменит уровни финансирования по всему, от военной помощи США Украине до Фонда модернизации технологий.

Лидер меньшинства в Палате представителей Кевин Маккарти, штат Калифорния, который может стать спикером, если республиканцы возьмут контроль над палатой, также дал понять, что Палата представителей отменит приток расходов IRS, введенный демократами. Сокращение финансирования в IRS может замедлить его шестилетнюю работу по модернизации ИТ, которая включает в себя улучшение обслуживания налогоплательщиков и капитальный ремонт устаревшей ИТ-инфраструктуры, и может изменить то, как агентство регулирует криптовалюту.

Маккарти также дал понять, что комитеты под руководством республиканцев расследуют реакцию администрации Байдена на COVID-19, министерство юстиции и вывод войск из Афганистана. Солоуэй сказал, что состав председателей комитетов в Палате представителей будет иметь ключевое значение для того, как Конгресс будет осуществлять надзор.

«Независимо от того, что происходит, смотрите на председателей комитетов, потому что в них сила», — сказал Солоуэй. «Будет много потасовок».

Конгресс теряет экспертизу кибербезопасности

Независимо от расы, которая все еще вызывает сомнения, Конгресс поделится значительным опытом в области политики кибербезопасности. Если демократы сохранят большинство в Палате представителей, палата все равно потеряет члена палаты представителей Джима Ланжевена, доктора медицины, в отставку. Имея ключевой пост в Комитете по вооруженным силам, а также руководя группой Конгресса по кибербезопасности и членством в Комиссии по солярию киберпространства, Ланжевен сыграл ключевую роль в продвижении множества двухпартийных положений в закон, в первую очередь создание офиса национальный кибер-директор.

Член палаты представителей Джон Катко, штат Нью-Йорк, и сенатор Роб Портман, штат Огайо, работавшие параллельно с демократами, также сыграли важную роль в получении дополнительных полномочий и увеличении бюджетов для Агентства кибербезопасности и безопасности инфраструктуры. Но оба также покидают Конгресс.

В более вероятном случае, если республиканцы возьмут палату представителей, и даже если преемник Катко, который возглавит Комитет внутренней безопасности, также захочет поддержать CISA, у руководства могут

быть другие идеи. Маккарти заявил, что планирует уделить первоочередное внимание борьбе с инфляцией, что может привести к сокращению расходов на кибербезопасность.

Сенатор Мэгги Хассан, DN.H., председатель подкомитета Сената по внутренней безопасности и делам правительства по возникающим угрозам и надзору за расходами, во вторник выиграла свою гонку против республиканского претендента Дональда Болдука. Хасан был ярым сторонником усиления федеральной политики кибербезопасности и, если демократы сохранят контроль Сената, может стать влиятельной фигурой в будущем обсуждении киберполитики.

Еще одним ярким моментом в промежуточных выборах прошлой ночью для сторонников кибербезопасности в Конгрессе стала победа члена палаты представителей Элиссы Слоткин в гонке округа 8 штата Мичиган. Слоткин, ветеран-конгрессмен и бывший аналитик ЦРУ, принимала активное участие как в демократических, так и в двухпартийных законодательных инициативах в области технологий. Законопроекты, которые она спонсировала, включают Закон CISA о киберупражнениях, который установит более строгий надзор за атаками на критически важную инфраструктуру и готовность, а также Закон о раскрытии информации и подотчетности ботов от 2019 года, который потребует от социальных сетей улучшить раскрытие информации о пользователях и учетных записях, не являющихся людьми.

Послужной список Слоткин также свидетельствует о том, что она поддерживает другие технологические инициативы, представленные на Холме, с ее участием в законопроектах, посвященных сельскому обучению STEM, исследованиям избирательных технологий и улучшению картирования широкополосной связи в сообществе.

Что это будет означать для FCC и FTC?

Администрация Байдена может больше полагаться на федеральные агентства, такие как Федеральная комиссия по связи и Федеральная торговая комиссия, в использовании своих нормотворческих полномочий во время раскола Конгресса. Например, Федеральная торговая комиссия в настоящее время рассматривает предложенный законопроект о конфиденциальности данных, но детали плана агентства на данный момент неясны.

Тупиковая ситуация в Конгрессе еще больше подчеркнет важность заполнения должностей в ключевых агентствах. Кроме того, изменения в комитетах, таких как комитет Палаты представителей по энергетике и торговле, который курирует FTC и FCC, могут изменить законодательные усилия и надзор. Комитет в настоящее время возглавляет член палаты представителей Фрэнк Паллоне, DN.J., но если республиканцы победят, член палаты представителей Кэти МакМоррис Роджерс, R-Wash., Скорее всего, возглавит комитет. Она разделяет цель FTC в отношении конфиденциальности, но заявляет, что она должна принадлежать Конгрессу, а не агентству.

«Конгресс подрезает им крылья?» Солоуэй сказал, предполагая, что Конгресс под руководством республиканцев может сократить основные политические решения, принимаемые независимыми агентствами.

Если Палата представителей перейдет под контроль республиканцев, технологические активисты ожидают серьезной технологической реформы.

«Если республиканцы возьмут верх над ключевыми комитетами, они попытаются замедлить работу Федеральной торговой комиссии и забросают ее механизм песком. Таким образом, активистам нужно будет держать агентство в центре внимания и потребовать, чтобы Лина Хан выступила против лицемерной оппозиции», — сказал Эван Грир, директор онлайн-адвокационной организации «Борьба за будущее», в комментариях, отправленных Nextgov.

Куда может быть направлена реформа Раздела 230

Обе политические партии в последние годы отстаивали реформу раздела 230. Этот язык является частью Закона о порядочности в общении 1996 года, который освобождает интернет-сервисы от ответственности за контент третьих лиц, опубликованный на их платформе, и это стало актуальной технической проблемой, поскольку дезинформация и дезинформация на социальных платформах стали частью избирательная норма. Раздел 230 эффективно устраняет ответственность основных онлайн-платформ, а именно Facebook, YouTube и Twitter, из риторики и материалов, распространяемых на их веб-сайтах.

Хотя у обеих политических партий есть проблемы с разделом 230, они по-разному стремятся их решать. Критически относясь к иммунитету Big Tech, демократы в целом считают, что правило препятствует необходимой модерации проблемного или оскорбительного контента в Интернете. Между тем, республиканцы нацелились на это положение, когда бывший президент Дональд Трамп попытался заставить Конгресс пересмотреть или отменить раздел 230, утверждая, что он допускает как распространение дезинформации, так и несправедливую цензуру консервативных материалов, публикуемых в социальных сетях.

Учитывая продолжающееся присутствие поддерживаемых Трампом кандидатов от Республиканской партии во многих штатах на полях сражений, вопросы больших технологий и цензуры также фигурировали на промежуточных выборах 2022 года. Один из примеров этого произошел в ходе кампании члена палаты представителей Лорен Боберт, R-Co., которая работает над тем, чтобы отбиться от претендента от демократов Адама Фриша на место в Палате представителей округа 3 штата.

Боеберт отметила свой первый срок в Конгрессе неизменной верностью платформам кампании Трампа, в том числе нацеленным на раздел 230. В этом году Боеберт выступила соавтором закона «Остановить цензуру», который внесет поправки в раздел 230, ограничив иммунитет компании, работающей в социальных сетях, за «проверку или блокировку» контента считается оскорбительным на своей платформе. Это особенно отличает тип контента, который является «незаконным», от «просто нежелательного», изменяя то, что может регулировать Раздел 230.

Хотя предвыборная гонка Боберта еще не объявлена, вполне вероятен республиканский контроль над палатой представителей. Грир отметил, что популярные технические вопросы, такие как конфиденциальность данных и модерация контента, будут пересекаться с другими законодательными темами, что будет иметь серьезные последствия для американцев.

«Что меня больше всего беспокоит, так это то, что тогда на председателей комитетов будет оказано сильное давление, чтобы они «нашли точки соприкосновения» между демократами и республиканцами по статье 230», — сказал Грир «Республиканцы думают, что изменение раздела 230 приведет к большей свободе слова в Интернете. Демократы считают, что изменение Раздела 230 приведет к тому, что платформы Big Tech будут лучше модерировать контент и разрабатывать свои платформы более безопасно. Они оба неправы». ***(Frank Konkel, Mariam Baksh, Kirsten Errick, Alexandra Kelley. Here's what a split Congress might mean for tech, cybersecurity and governance // Nextgov (https://www.nextgov.com/technology-news/2022/11/what-divided-government-could-mean-tech-policy/379534/). 09.11.2022).***

***

«Генеральные инспекторы из торговли и казначейства рассказывают о двух режимах тестирования.

В отдельных отчетах наблюдательные органы агентства продемонстрировали разницу, которую может иметь надлежащее внедрение средств контроля обнаружения в ограничении воздействия попыток кибервторжений: во-первых, предотвращенная атака программы-вымогателя против Службы внутренних доходов; другой — внутренний тест на проникновение устойчивости Бюро переписи населения.

Согласно отчету от 23 ноября, сотрудники IRS сообщили генеральному инспектору Министерства финансов по налоговой администрации, или TIGTA, что их централизованный центр информационной безопасности отреагировал и нейтрализовал атаку программы-вымогателя, обнаруженную в мае.

В отчете TIGTA отмечается успешное обнаружение и реагирование на процедуры тестирования, которые IRS включила в свою политику в соответствии с рекомендациями Национального института стандартов и технологий и Агентства по кибербезопасности и безопасности инфраструктуры.

В другом отчете генерального инспектора — от Министерства торговли — показано, как неполная реализация аналогичной политики может привести к совершенно разным результатам, в данном случае в Бюро переписи населения.

Бюро переписи населения обязано «записывать и отслеживать активность в своей сети и реагировать на предупреждения о потенциальных инцидентах безопасности», но не смогло этого сделать, как написала Commerce IG в отчете от 22 ноября, основанном на проведенном скрытом тесте на проникновение. с августа 2021 года по март текущего года.

Commerce IG провела тест в ответ на атаку на Бюро переписи населения в январе 2020 года, в ходе которой злоумышленники извне успешно воспользовались дырами в безопасности. Во время недавних учений «красная команда» Commerce IG смогла избежать обнаружения, получив доступ к информации, позволяющей установить личность, или PII, хранящейся в Бюро переписи населения.

Commerce IG предложила агентству установить «процесс периодического тестирования и проверки веб-сайтов и веб-приложений Бюро на наличие уязвимостей и подверженности злонамеренному вводу», наряду с другими рекомендациями, с которыми согласилось Бюро переписи населения.

Напротив, у IG Министерства финансов не было рекомендаций для IRS. В этом отчете описана активная и комплексная система реагирования на признаки злонамеренного поведения в Центре реагирования на инциденты компьютерной безопасности IRS.

«CSIRC обеспечивает ежедневный оперативный мониторинг и анализ попыток вторжения или аномальной активности», — пишет IG, отмечая, что отчеты «оцениваются для определения характера и серьезности событий, чтобы сформулировать оперативный ответ для сдерживания и ликвидации, тем самым сводя к минимуму воздействие. Сообщенные инциденты документируются в централизованной системе отслеживания инцидентов CSIRC и дополнительно сортируются для определения достоверности, серьезности и воздействия события».

Согласно отчету, в случае майского инцидента с программой-вымогателем сотрудники CSIRC обнаружили закономерности в своем анализе журналов просмотра веб-страниц, которые предполагали наличие программы-вымогателя, и смогли найти и вытащить затронутое устройство из сети.

С другой стороны, IG Commerce «обнаружила, что, хотя вредоносная активность в основном фиксируется в журналах… Бюро [переписи] не настроило свои инструменты безопасности для генерации предупреждений об этих конкретных индикаторах атак и действий», что позволило Red Teams остаться незамеченным.

Commerce IG дала 10 рекомендаций Бюро переписи населения, в том числе следующее: «Разрабатывайте оповещения, соответствующие общим методам обнаружения известных атак, и периодически проверяйте, чтобы эти методы обнаружения оставались актуальными и эффективными [и]… Обновляйте требования к конфигурации ведения журналов для сбора необходимой информации». для сообщения о нарушениях, связанных с конфиденциальной PII». ***(Mariam Baksh. What the Census Bureau Can Learn From the IRS About Detecting Cyberattacks // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/what-census-bureau-can-learn-irs-about-detecting-cyberattacks/380217/). 28.11.2022).***

***

«Запрос поможет агентству разработать платформу для решения текущих задач, связанных с анализом киберугроз.

Администрация общих служб подала запрос на предоставление информации от имени Агентства по кибербезопасности и безопасности инфраструктуры о наличии корпоративных служб Threat Intelligence (или TIES), чтобы помочь агентству в разработке возможностей разведки киберугроз (или CTI).

По данным CISA, существуют существующие барьеры для федеральной киберэкосистемы на протяжении всего жизненного цикла CTI, такие как фрагментированная информация об угрозах, которая влияет на способность аналитиков эффективно принимать обоснованные решения об этих рисках, а также CTI, существующие в настоящее время в различных потоках в разных данных. форматы. Участники этой среды обмена разведывательными данными также имеют различные уровни киберзрелости.

CISA добавила, что федеральной киберэкосистеме необходимо улучшить инструменты и услуги CTI и их закупку, одновременно разрабатывая оценки

зрелости CTI и дорожные карты. Экосистема также должна обеспечить осведомленность и централизацию требований CTI. В результате CISA работает над созданием TIES для предоставления клиентам услуг CTI, стандартов и руководств, связанных с созданием, использованием и обменом CTI.

RFI в четверг поможет правительству провести исследование рынка, чтобы определить потенциальные предложения и получить отзывы от отрасли. Как отмечается в RFI, представители отрасли помогут разработать или настроить платформу обмена информацией о киберугрозах, а затем интегрировать ее с настроенными приложениями CISA и каналом для коммерческих угроз. Возможности разведки киберугроз будут «предлагаться в виде набора корпоративных услуг федеральным, разведывательным сообществам, государственным и правоохранительным органам».

В частности, воображаемая платформа обмена предоставит заинтересованным сторонам упрощенный ввод и совместное использование CTI в качестве «единой точки интеграции для аналитиков и инфраструктуры, чтобы получать, обмениваться и совместно работать над актуальными и своевременными CTI, позволяя командам защищать свою среду и других», согласно РФИ. В частности, платформа будет принимать и агрегировать CTI из автоматического обмена индикаторами CISA, коммерческих каналов информации об угрозах и других источников. Платформа CTI позволит аналитикам сотрудничать, а клиентам использовать централизованную совместимую платформу для проверки CTI на предмет рисков кибербезопасности.

Согласно RFI, платформа должна: поддерживать формат обмена данными Structured Threat Information Expression, или STIX, и механизм передачи данных Trusted Automated Exchange of Intelligence Information, или TAXII; предоставить REST API — или репрезентативную передачу состояния — чтобы разрешить внешним клиентам автоматический доступ к данным и рабочим процессам на платформе; позволяют принимать, маркировать и коррелировать несколько наборов данных, связанных с угрозами; и поддерживать собственные типы данных для объектов домена STIX в дополнение к возможности индексировать и запрашивать такие объекты…». ***(Kirsten Errick. CISA Seeks Information for Potential Cyber Threat Intelligence Platform // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/cisa-seeks-information-potential-cyber-threat-intelligence-platform/380020/). 21.11.2022).***

***

«Руководство содержит рекомендации на протяжении всего жизненного цикла продукта, от закупки до развертывания.

Несколько агентств опубликовали последнюю часть серии о безопасности цепочки поставок программного обеспечения, на этот раз сосредоточив внимание на клиентах.

Руководство, выпущенное в четверг Агентством кибербезопасности и безопасности инфраструктуры, Агентством национальной безопасности и Управлением директора национальной разведки, дает рекомендации для клиентов программного обеспечения «для обеспечения целостности и безопасности программного обеспечения на этапах закупки и развертывания».

Агентства предоставляли рекомендации на протяжении всего жизненного цикла программного обеспечения, включая: определение требований, оценку продукта, контракты, развертывание, тестирование, интеграцию, развертывание продукта, обновления и обучение.

Например, рекомендации включают: своевременное обновление оценок безопасности и рисков, обеспечение достаточной защиты и контроля геолокационных данных и метаданных; и, среди прочего, определение и назначение отдельных ролей.

Это руководство для клиентов следует аналогичному августовскому документу для разработчиков и октябрьскому руководству для поставщиков. Однако отчет для разработчиков был встречен неоднозначными отзывами со стороны отрасли…». ***(Kirsten Errick. Latest Guidance Outlines Customer Responsibilities for Software Security // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/latest-guidance-outlines-customer-responsibilities-software-security/379945/). 18.11.2022).***

***

«Управление управления и бюджета выпустило новое руководство, чтобы начать общегосударственные усилия по защите цифровой инфраструктуры от квантовых атак.

Административно-бюджетное управление Белого дома опубликовало новый меморандум, в котором излагается необходимость того, чтобы федеральные агентства начали переход на постквантовую криптографию до появления операционных квантовых компьютеров.

Подготовительные меры OMB рекомендует федеральным органам последовать примеру более раннего указа президента Джо Байдена об усилении киберзащиты США. В новом меморандуме устанавливаются требования к федеральным агентствам по инвентаризации их текущих криптографических аппаратных и программных систем с акцентом на ценные активы и системы с высокой степенью воздействия, которые требуют дополнительных протоколов кибербезопасности.

Затем руководству агентства будет поручено собрать эту информацию в отчет, содержащий их индивидуальные сводки по информационным активам и системам с более высоким риском, для Управления национального кибер-директора и Агентства по кибербезопасности и безопасности инфраструктуры, чтобы помочь составить бюджет, спланировать и выполнить переход от стандарта. эффективной постквантовой криптографии.

Чиновники OMB уточняют, что системы высокого риска, представленные агентствами, будут в первую очередь обрабатывать конфиденциальные данные, которые могут быть использованы любыми попытками квантового взлома.

«Администрация Байдена-Харриса работает над тем, чтобы обеспечить лидерство США в развивающейся области квантовых вычислений», — заявил Крис ДеРуша, федеральный директор по информационной безопасности, в заявлении Nextgov. «Эта глобальная технологическая гонка таит в себе как большие перспективы, так и угрозы. Мы отдаем приоритет нашим усилиям по защите конфиденциальных данных федерального правительства от возможного будущего

компрометации с помощью квантовых компьютеров; это действие знаменует собой начало крупного мероприятия по подготовке нашей страны к рискам, связанным с этой новой технологией».

У агентств будет время до 4 мая 2023 года, чтобы выполнить запрос OMB. В течение 30 дней после публикации меморандума агентствам будет поручено назначить ответственного за сбор информации о криптографических системах. OMB продолжит выпускать инструкции по сбору инвентаризации систем.

Согласно заявлению OMB, направленному в Nextgov, переход на постквантовые криптографические стандарты будет самым значительным на сегодняшний день и займет несколько лет. В течение года после публикации этого нового меморандума CISA поможет выпустить новые стратегии миграции совместно с Национальным институтом стандартов и технологий и Агентством национальной безопасности.

OMB рекомендовало федеральным агентствам при инвентаризации своих информационных систем сотрудничать с поставщиками программного обеспечения, чтобы определить возможности пост-квантового криптографического тестирования в своих сетях, говоря о стремлении администрации Байдена к сотрудничеству между государственным и частным секторами.

Несколько федеральных агентств работают в тандеме, чтобы продвигать постквантовую миграцию в государственных цифровых сетях. NIST ранее выпустил четыре квантово-устойчивых алгоритма для облегчения и ускорения обновления текущего кода. Они станут частью текущей инициативы NIST по постквантовой криптографии, которая, как ожидается, будет завершена в течение двух лет». ***(Alexandra Kelley. White House Begins to Push Federal Post-Quantum Cryptography Migration // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/white-house-begins-push-federal-post-quantum-cryptography-migration/379936/). 18.11.2022).***

***

«В новом руководстве федеральных агентств и крупных компаний, обслуживающих правительство, делается попытка провести различие между обязанностями по обеспечению безопасности разработчиков, поставщиков и потребителей программного обеспечения.

Поставщики программного обеспечения несут уникальную ответственность за обеспечение эффективной доставки своих продуктов с учетом рисков безопасности, согласно руководству, недавно выпущенному Агентством национальной безопасности совместно с Агентством кибербезопасности и безопасности инфраструктуры.

«Предотвращение часто рассматривается как обязанность разработчика программного обеспечения, поскольку от него требуется безопасная разработка и доставка кода, проверка сторонних компонентов и укрепление среды сборки», — говорится в пресс-релизе АНБ от 31 октября. «Но поставщик также несет серьезную ответственность за обеспечение безопасности и целостности нашего программного обеспечения. В конце концов, поставщик программного обеспечения отвечает за связь между заказчиком и разработчиком программного обеспечения. Именно благодаря этим отношениям могут применяться дополнительные функции

безопасности посредством договорных соглашений, выпусков и обновлений программного обеспечения, уведомлений и устранения уязвимостей».

Документ, предназначенный для поставщиков программного обеспечения, является одним из трех. Enduring Security Framework, в которую входят официальные лица правительства США, а также представители отрасли информационных технологий, связи и обороны, выпустила руководство для разработчиков в сентябре и планирует в дальнейшем решать вопросы безопасности потребителей программного обеспечения.

Передовые методы обеспечения безопасности для производителей и пользователей программного обеспечения уже сформулированы, в первую очередь в «Структуре безопасной разработки программного обеспечения» Национального института стандартов и технологий, которую NIST использовал для выполнения своих обязательств по предоставлению рекомендаций для федеральных агентств в соответствии с указом президента 14028.

Президент Джо Байден издал приказ в мае 2021 года в ответ на событие SolarWinds, когда клиенты вездесущей фирмы по управлению ИТ были скомпрометированы после установки того, что казалось обычным обновлением. Хакеры получили несанкционированный доступ к механизму доставки SolarWinds и замаскировали свое вредоносное ПО новым кодом.

«Эта серия поможет наладить взаимодействие между этими тремя разными ролями и между специалистами по кибербезопасности, что может способствовать повышению отказоустойчивости и безопасности в процессе цепочки поставок программного обеспечения», — говорится в документе, в котором не уточняется различие между разработчиками программного обеспечения и поставщиками программного обеспечения.

В приказе Байдена подчеркивалась ответственность агентств за тщательную проверку приобретаемого ими программного обеспечения, а Управление по вопросам управления и бюджета требовало от должностных лиц по закупкам собирать форму, которую должны создать CISA, которую поставщики программного обеспечения могут подписать, чтобы подтвердить соблюдение практик, указанных в руководство НИСТ. Приложение, включенное в документ, предполагает, что разработчики должны нести основную ответственность за внедрение этих практик, а поставщики должны нести основную ответственность за проверку их эффективности». ***(Mariam Baksh. CISA, NSA and Industry Outline Security Responsibilities of Software Suppliers // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/cisa-nsa-and-industry-outline-security-responsibilities-software-suppliers/379423/). 07.11.2022).***

***

«Фирма по кибербезопасности Recorded Future выявила кампании дезинформации, предполагающие, что машины для голосования от трех крупных компаний «будут использоваться для фальсификации результатов промежуточных выборов».

Ложные заявления о точности машин для голосования, которые распространились в социальных сетях и альтернативных новостных платформах

после президентских выборов 2020 года, вероятно, увеличатся после промежуточных выборов во вторник, согласно отчету, опубликованному Insikt Group компании Recorded Future в понедельник.

В отчете «Мистификация в машине: дезинформация против производителей и технологий систем голосования на промежуточных выборах в США в 2022 году» рассматривается ложь о производителях систем голосования — или VSM — «созданная в период между всеобщими выборами 2020 года и промежуточными выборами 2022 года».

Аналитики Recorded Future обнаружили, что многие заявления о точности машин для голосования были направлены на три основных VSM: Dominion Voting Systems, Smartmatic и Election Systems & Software. Как отмечается в отчете, все три компании столкнулись с необоснованными обвинениями в фальсификации выборов после выборов 2020 года. Dominion и Smartmatic подали несколько исков о клевете против союзников бывшего президента Дональда Трампа и правых СМИ за то, что они утверждали, что их машины были сфальсифицированы в пользу президента Джо Байдена.

«Recorded Future уже выявила утверждения по многочисленным аспектам основного и альтернативного ландшафта социальных сетей, предполагающие, что технологии, развернутые вышеупомянутыми компаниями, будут использоваться для фальсификации результатов промежуточных выборов», — говорится в отчете.

Большая часть ложной и дезинформации, нацеленной на VSM, указанную в отчете, была «концентрирована на крайне правых и ультраконсервативных альтернативных платформах социальных сетей и «новостных» блогах» и включала заявления о том, что машины для голосования компаний удаляли или подменяли голоса, или работали в тандеме с федеральными агентствами для фальсификации результатов выборов. Аналитики Recorded Future обнаружили, что многие из ложных сведений о трех VSM, которые были распространены после выборов 2020 года, продолжают распространяться в различных социальных сетях в преддверии промежуточных выборов, в том числе на основных платформах, таких как Facebook и Telegram, а также на больше второстепенных сайтов, таких как форумы Gab, 4chan и Qanon.

В отчете также говорится, что Scytl — VSM со штаб-квартирой в Испании, чьи технологии не использовались ни на каких выборах в США в 2020 г. и не будут использоваться в промежуточных выборах 2022 г., — «имела чрезмерное присутствие среди теорий заговора из-за обвинений в подсчете голосов за границей с участием Компании».

Хотя в отчете отмечается, что «подавляющее большинство ложной информации, нацеленной на VSM, скорее всего, исходит из внутренних источников в США, а не из-за иностранного влияния», аналитик из Insikt Group Recorded Future сказал Nextgov, что иностранные субъекты как открыто, так и тайно усиливают эту ложную информацию через государственные СМИ и скрытые пропагандистские аккаунты в социальных сетях.

«Скорее всего, влиятельные лица из числа национальных государств отслеживают ложные информационные нарративы в Интернете и, если они пользуются популярностью, согласовывают свои собственные усилия по влиянию с

этими нарративами», — сказал аналитик Recorded Future. «Это верно независимо от того, исходят ли нарративы от влиятельных лиц национального государства или от внутренней аудитории. Если повествование о «сфальсифицированных машинах для голосования» продолжится после промежуточных выборов в США, что почти наверняка произойдет, то мы, вероятно, увидим, как влиятельные лица из национальных государств, особенно из России, будут повторять и дополнять это повествование в будущем».

В предыдущем отчете, опубликованном Recorded Future 13 октября, говорилось, что противники из числа национальных государств, включая Китай, Иран и Россию, а также внутренние экстремисты были вовлечены в кампании злонамеренного влияния, направленные на среднесрочные выборы 2022 года.

Независимо от их происхождения, эти утверждения о фальсификации машин для голосования, вероятно, вызовут наибольший резонанс в ходе ожесточенных споров в Палате представителей, Сенате и губернаторских выборах. Хотя в отчете отмечается, что «ни одна избирательная юрисдикция не застрахована от дезинформации VSM», в нем говорится, что некоторые штаты, являющиеся полем боя, включая Аризону, Флориду, Джорджию, Неваду, Пенсильванию и Висконсин, «наиболее вероятно, будут объектами постоянных усилий по дезинформации VSM». во время и после промежуточных выборов 2022 года.

«Управляющие избирательными участками в таких юрисдикциях должны быть готовы к чрезмерной проверке как используемых технологий голосования, так и самих администраторов в связи с функционированием этих технологий», — говорится в отчете.

Учитывая количество противников выборов, баллотирующихся на государственные должности в промежуточные сроки (в октябрьском отчете Института Брукингса было выявлено 345 кандидатов на государственные и федеральные должности, «которые выразили убеждение в отрицании выборов»), увеличение числа избранных должностных лиц, продвигающих ложные заявления о фальсифицированные машины для голосования также могут продолжать подрывать доверие к избирательному процессу.

«Меня беспокоит то, что некоторые из этих отрицателей выборов уже отказались сказать, примут ли они результаты выборов, если они проиграют, и что, поскольку у них есть последователи, они будут использовать нарратив о том, что машины для голосования используются для «исправления ошибок». «выборы», — сказал аналитик Recorded Future. «Это, вероятно, увеличит количество людей, которые верят этому рассказу, и может придать ему импульс перед выборами 2024 года».

И продолжающееся продвижение этой лжи может иметь как внутренние, так и глобальные последствия. В отчете говорится, что «отрицание выборов в США и дезинформация VSM наносят ущерб демократическому миру в целом», особенно потому, что три VSM, указанные в отчете, «вероятно, продолжат сталкиваться с эхом американских заговоров относительно их технологий голосования на других выборах по всему миру».

Для многих киберэкспертов ложная и дезинформация о системах голосования в США представляет большую угрозу для избирательного процесса, чем риск

кибератак на избирательную инфраструктуру. В частности, злоумышленники все чаще нацеливают свои ложные заявления на различные и неанглоязычные сообщества, что требует более активного участия федеральных чиновников и даже некоторых некоммерческих организаций.

Агентство по кибербезопасности и безопасности инфраструктуры и ФБР ранее выпустили в октябре два совместных заявления государственной службы, в которых излагались некоторые средства контроля безопасности выборов, действующие для защиты систем голосования от вторжения извне, и описывалось, как иностранные субъекты могут использовать тактику манипулирования, «направленную на подрывать доверие к избирательным процессам и влиять на общественное мнение о легитимности выборов». CISA также создала веб-сайт «Слухи против реальности» для борьбы с ложными утверждениями о результатах выборов и рекомендовала американской общественности обращаться за рекомендациями и информацией, касающимися голосования, к официальным представителям избирательных комиссий штата и местных органов власти». ***(Edward Graham. Voting Machine Myths Likely to Increase During and After Midterms, Report Finds // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/voting-machine-myths-likely-increase-during-and-after-midterms-report-finds/379409/). 07.11.2022).***

***

«Уведомление о предлагаемом нормотворчестве потребует от участников системы экстренного оповещения сообщать о кибер-нарушениях в течение 72 часов после их обнаружения.

Федеральная комиссия по связи недавно проголосовала за утверждение уведомления о предлагаемом нормотворчестве, которое направлено на повышение кибербезопасности национальной системы оповещения населения, частично требуя, чтобы операторы системы оповещения о чрезвычайных ситуациях (или EAS) сообщали о любых нарушениях своего оборудования в агентство в течение 72 часов.

Предложение, принятое Федеральной комиссией по связи 27 октября 4:0, требует, чтобы участники системы «сообщали о любом случае несанкционированного доступа к своему оборудованию EAS» в комиссию в течение трех дней с того момента, «когда она узнала или должна была стало известно о происшествии». Участники EAS должны будут уведомить агентство в течение этого периода времени и предоставить информацию о нарушении, независимо от того, «привел ли этот взлом к передаче ложного предупреждения».

Системы EAS и беспроводного оповещения о чрезвычайных ситуациях (или WEA) используются для передачи информации о чрезвычайных ситуациях населению, часто в ответ на суровые погодные условия, стихийные бедствия или пропажу детей. Оповещения, которые издаются местными, государственными и федеральными властями, доставляются по радио, телевидению и мобильным текстовым сообщениям.

«Мы считаем, что предлагаемое правило оправдано в свете случаев ложных предупреждений EAS в последние годы, вызванных скомпрометированным оборудованием EAS, используемым для передачи ложных сообщений», — говорится в уведомлении FCC о предлагаемом нормотворчестве.

Голосование было проведено после того, как 1 августа Федеральное агентство по чрезвычайным ситуациям опубликовало предупреждение об «определенных уязвимостях в устройствах кодировщика/декодера EAS, которые, если не будут обновлены до самых последних версий программного обеспечения, могут позволить субъекту выдавать предупреждения EAS через инфраструктуру хоста. (ТВ, радио, кабельная сеть)».

Предыдущие инциденты — как преднамеренные, так и непреднамеренные — подчеркнули панику, которая может быть вызвана ложными оповещениями о чрезвычайной ситуации. В январе 2018 года сотрудник службы управления чрезвычайными ситуациями Гавайев по ошибке разослал предупреждение, в котором жителям предупредили искать укрытие от приближающейся баллистической ракеты. А в 2020 году местная система аварийного оповещения кабельного телевидения в штате Вашингтон была взломана хакером, который разослал ложные предупреждения о радиационной аварийной ситуации.

В дополнение к ужесточению требований к сообщениям о нарушениях для участников EAS, предлагаемое правило также потребует, чтобы участники EAS и коммерческие поставщики мобильных услуг, которые являются частью системы WEA, «ежегодно подтверждали наличие плана управления рисками кибербезопасности и применяли достаточный уровень безопасности». меры по обеспечению конфиденциальности, целостности и доступности их соответствующих систем оповещения».

В своем заявлении комиссар FCC Джеффри Старкс процитировал данные, собранные Бюро общественной и национальной безопасности агентства во время общенационального тестирования EAS в августе 2021 года, которое показало, что «более 5000 участников EAS использовали устаревшее программное обеспечение или использовали оборудование, которое больше не поддерживает обычные программные обновления."

Старк также похвалил предложенное нормотворчество за получение общественного мнения о том, следует ли также требовать от участников WEA сообщать в FCC о несанкционированном доступе к их системам и оборудованию.

«Это важный шаг, — сказал Старк. «Без уведомления несанкционированный доступ может продолжаться беспрепятственно и распространяться на другие системы EAS и WEA».

Председатель FCC Джессика Розенворсель также заявила в своем заявлении, что нормотворчество агентства необходимо для повышения оперативной готовности национальных систем оповещения населения.

«Эти усилия помогут обеспечить функционирование этих важных систем в чрезвычайных ситуациях и доверие общественности к предупреждениям, которые они получают», — сказал Розенворсель. «Это важно, потому что Министерство внутренней безопасности недавно определило, что некоторые из этих систем оповещения подвержены серьезным уязвимостям в системе безопасности. Хотя были выпущены некоторые исправления для исправления этих недостатков, не все их установили. Мы стремимся исправить это здесь и сейчас».

Во время октябрьского мероприятия, организованного Washington Post, заместитель советника по национальной безопасности Энн Нойбергер упомянула

усилия FCC по снижению риска киберугроз для систем оповещения населения как один из компонентов усилий администрации Байдена по укреплению цифровой безопасности критически важной инфраструктуры страны. сектора.

Уведомление FCC о предлагаемом нормотворчестве открыто для общественного обсуждения через 30 дней после объявления правила 27 октября и в общей сложности 60 дней для ответов на комментарии. Затем агентство проголосует за принятие правил». ***(Edward Graham. FCC Proposes to Strengthen Cybersecurity of Emergency Alert Systems // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/fcc-proposes-strengthen-cybersecurity-emergency-alert-systems/379367/). 04.11.2022).***

***

«Выборы 2020 года прошли успешно без каких-либо серьезных сбоев, но это не помешало некоторым людям усомниться в легитимности выборов и существующих методах безопасности для их защиты. И хотя утверждения о несправедливых или предвзятых выборах были почти полностью опровергнуты, по-прежнему крайне важно изучить кибербезопасность и другие средства защиты, связанные с голосованием, чтобы защитить будущие выборы, подобные тем, которые состоятся всего через несколько дней.

Nextgov поговорил с двумя экспертами по кибербезопасности о безопасности выборов. Они указали как на сильные стороны существующей системы, так и на некоторые потенциальные уязвимые места, которых правительственным чиновникам следует опасаться в будущем.

Марк Стэмфорд — основатель и генеральный директор OccamSec, фирмы по кибербезопасности, которая помогает организациям проводить непрерывное тестирование на проникновение в свои сети. Но Стэмфорд начал свою карьеру не в белой шляпе. До этого он был хакером.

Nextgov: Прежде чем мы начнем, не могли бы вы немного рассказать нам о своем личном опыте и о том, как вы начали изучать безопасность наших выборов и других критически важных сетей и инфраструктуры?

Стэмфорд: Конечно. Я начал возиться с безопасностью, когда был маленьким, потому что это казалось забавным занятием. Оттуда я стал профессиональным тестером на проникновение. Затем, около 11 лет назад, я основал компанию OccamSec, которая изначально занималась тестированием на проникновение и Red Teaming. Первоначально это был только я, но мы расширились, включив в себя разведывательную поддержку и поиск угроз.

Nextgov: Во-первых, если посмотреть на предыдущие выборы в 2020 году, были ли предприняты какие-либо заметные атаки или попытки взлома систем голосования?

Стэмфорд: Я думаю, что самой большой атакой была социальная инженерия избирателей с помощью кампаний по дезинформации, что было действительно самым большим взломом из всех. И это имеет смысл, если подумать о том, что социальная инженерия продолжает оставаться чрезвычайно эффективным вектором. Платформы социальных сетей были превращены в оружие, а создаваемые ими эхо-камеры манипулировались с большим успехом.

С точки зрения крупномасштабной атаки, направленной непосредственно на систему голосования, это все еще было сложной задачей для злоумышленников. США не похожи на некоторые другие страны, где люди могут голосовать онлайн в больших количествах. И учитывая то, что произошло в 2020 году, кажется, что мы наблюдаем негативную реакцию против реализации этого.

Nextgov: Заглядывая вперед, поскольку вы можете видеть обе стороны забора с точки зрения кибербезопасности, думаете ли вы, что уязвимости в системе безопасности станут проблемой для предстоящих выборов, которые состоятся всего через несколько дней?

Стэмфорд: Это не будет слишком большой проблемой для следующих выборов, но для 2024 года вполне может. Неизбежно, что все больше систем голосования будет переведено в онлайн, а удаленные возможности будут расширены. Если холодильник подключен к Интернету, чтобы сообщать вам, когда у вас закончилось молоко, вероятно, скоро появится онлайн-система голосования, чтобы вы могли голосовать, а администраторы могли решать проблемы в два часа ночи в воскресенье. Это, в свою очередь, усилит внимание наших противников к попыткам компрометации этих систем.

Nextgov: Глядя на будущие выборы, какие ключевые области необходимо учитывать при разработке кибербезопасности выборов, чтобы предотвратить наиболее вероятные пути потенциальной атаки?

Стэмфорд: На данный момент локальные атаки, вероятно, по-прежнему являются основным направлением атак, что похоже на внутренний тест на проникновение, особенно с учетом использования беспроводных сетей и фрагментарного характера нашей системы голосования. Вполне вероятно, что в средах опроса будут использоваться беспроводные сети, которые злоумышленники попытаются скомпрометировать как можно дальше.

В то же время социальная инженерия избирательных комиссий усилится. Если злоумышленник может заставить администратора выдать свой пароль, это значительно упрощает доступ к системам.

Удаленные атаки — исходящие из-за пределов действия беспроводного сигнала или даже из другой страны — это, конечно, то, что получает больше внимания в прессе, но онлайн-голосование все еще находится в зачаточном состоянии. Так что на данный момент я думаю, что такая потенциальная атака скорее исключение.

Другой вектор — это то, что теперь известно как атаки на цепочку поставок. Что, если злоумышленник сможет скомпрометировать программное обеспечение, которое входит в систему голосования? Или какое-то программное обеспечение, выполняющее вспомогательную роль? В этом случае вы столкнетесь с проблемой типа SolarWinds, когда агент, развернутый в системе, на самом деле является источником проблемы.

Nextgov: Интересно, что Стэмфорд называет социальную инженерию и использование социальных сетей потенциальной уязвимостью перед выборами. Социальные сети существуют за пределами какой-либо сети, предназначенной для голосования, и тем не менее могут влиять на избирателей и выборы без

необходимости прямого взлома. Это вопрос, который изучает наш следующий эксперт, Мэтт Чиоди.

Мэтт, можешь сначала немного рассказать нам о себе?

Чиоди: Мое увлечение кибербезопасностью началось в нежном восьмилетнем возрасте, когда родители купили мне TRS-80 в RadioShack. Я был очарован машиной, которую можно было запрограммировать на то, что я ей скажу. Пожалуй, еще более интересным для меня было то, как его сломать. С годами я все больше и больше интересовался тем, как работают компьютеры, узнавая массу информации о хакерстве из древней среды, известной как BBS — система доски объявлений. В колледже я провел много времени, исследуя университетские сети, исследуя уязвимости, находя их и используя их. После колледжа я начал работать системным администратором Unix и быстро переключился на кибербезопасность, где провел последние 20 лет.

Nextgov: А теперь вы работаете с охранной фирмой Cerby. Что побудило вас присоединиться к ним?

Чиоди: Я присоединился к Cerby, потому что они решали проблему, на которую больше никто даже не смотрел. Основатели обнаружили огромный класс приложений, используемых правительствами и предприятиями по всему миру, которые не соответствуют общепринятым стандартам безопасности, таким как единый вход. Мы называем эту группу «неуправляемыми приложениями», потому что на предприятии это именно то, чем они являются... неуправляемыми.

Nextgov: Хорошо, давайте поговорим о социальных сетях с точки зрения безопасности выборов. Марк говорит, что это очень тревожная область. Почему социальные сети представляют собой потенциальную угрозу выборам?

Чиоди: Потому что повлиять на голосование гораздо проще, чем напрямую изменить его в избирательной системе — по крайней мере, в Соединенных Штатах. Каждое национальное государство имеет неутолимый аппетит к данным. Учтите, что США были крупнейшим запросчиком данных для многих из самых популярных платформ социальных сетей. Не думайте о данных одной платформы социальных сетей изолированно, но что может сделать с ними национальное государство в сочетании с данными из общедоступных источников и источников даркнета, таких как взлом Twitter несколько месяцев назад, который разоблачил миллионы его пользователей?

Любое национальное государство, имеющее доступ к этому объему данных, может использовать его в следующих реальных сценариях:

Они могли бы разрабатывать целевые кампании для выявления тех, кто имеет доступ к конфиденциальной интеллектуальной собственности, и проводить фишинговые кампании для получения доступа. Например, если вы работаете на оборонного подрядчика или в телекоммуникационной компании, вы можете стать главной мишенью.

Они могли повлиять на мнение группы пользователей, продвигая определенную точку зрения, выгодную для геополитической судьбы национального государства и его союзников. Скорее всего, это будет сделано с помощью алгоритма, который рекомендует видео.

Они могли бы создать долгосрочную кампанию, чтобы однозначно определить людей, которые, по их прогнозам, будут иметь наибольшее влияние в будущем в промышленности или обществе. Прогнозы могут быть основаны на различных степенях разделения, среди прочих факторов. На этих людей можно было бы нацеливаться и оказывать на них влияние в течение многих лет, а затем, в конечном итоге, к ним можно было бы обратиться в целях шпионажа.

Nextgov: Вау, это какой-то зловещий звук. Делало ли какое-либо национальное государство что-то подобное?

Чиоди: Хотя это и не пример национального государства, которое, скорее всего, будет рассекречено лишь в далеком будущем, примерно в это же время два года назад были взломаны некоторые очень известные аккаунты в Твиттере. Звезды, от бывшего президента Барака Обамы и Майкла Блумберга до Уоррена Баффета и Канье Уэста, с общей аудиторией в 250 миллионов человек, внезапно призвали своих последователей покупать биткойны по зловещим адресам. Твиттер узнал о проблеме только после того, как было опубликовано рекламное объявление. Вмешались правоохранительные органы, и оказалось, что подлыми преступниками оказались… подростки.

Nextgov: И этот инцидент, наряду с общими проблемами кибербезопасности, побудил вашу фирму провести аудит кибербезопасности ведущих платформ социальных сетей. Этот отчет скоро будет опубликован, но не могли бы вы дать нам краткий обзор некоторых ваших выводов?

Чиоди: Платформы социальных сетей, используемые популярными политическими лидерами США, часто не имеют средств контроля безопасности, необходимых для предотвращения кампаний по дезинформации. Политики США увеличили свое присутствие в обществе за последние несколько президентских выборов, следуя общей тенденции ухода от средств массовой информации, и национальные государства обратили на это внимание. В преддверии среднесрочной перспективы 2022 года Cerby оценил пять известных платформ социальных сетей на предмет контроля безопасности в критически важных областях, таких как двухфакторная аутентификация, готовность предприятия и конфиденциальность.

Несмотря на историю разногласий, Facebook занял первое место с общим баллом 2,85 из 5 возможных. Twitter занял второе место с показателем 2,78. Третье место занял Instagram с 2,27, за ним следует Reddit с 1,92 и TikTok с отдаленным 1,08. Обратите внимание, что эти платформы постоянно меняются и выпускают новые функции, и это была оценка на момент времени с осени 2022 года.

Nextgov: Каковы были самые большие различия между платформами с самым высоким рейтингом и самыми низкими?

Чиоди: Самым большим отличием, и где мы уделили наибольшее внимание, была сила вариантов двухфакторной аутентификации. Большинство потребителей рассматривают 2FA как единую технологию, хотя на самом деле существуют разные уровни безопасности с различными вариантами 2FA. Хотя такие платформы, как Facebook и Twitter, стоят на голову выше TikTok, их всех объединяет то, что ни одна из этих платформ не предлагает безопасность корпоративного уровня, кроме 2FA.

Даже в категории 2FA поддержка новых стандартов, таких как FIDO2 и U2F (без пароля), очень непоследовательна на платформах социальных сетей. Это

серьезная проблема, поскольку отсутствие вариантов аутентификации корпоративного уровня делает политических лидеров уязвимыми для атак с повторным использованием учетных данных. Политики США на этих платформах должны управлять своими паролями и, надеюсь, используют 2FA. Но предположим, что эти платформы предлагают поддержку параметров аутентификации корпоративного уровня, таких как единый вход? В этом случае политикам больше не нужно будет управлять своими паролями. Они могли положиться на свои армии ИТ-специалистов благодаря интеграции с популярными решениями для управления идентификацией, такими как Okta и Microsoft Azure Active Directory.

Nextgov: Хорошо, но как насчет дезинформации, которую часто называют угрозой выборам. Действительные учетные записи могут контролироваться национальными государствами с целью распространения дезинформации. Что мы можем с этим поделать?

Киоди: Дезинформация работает лучше всего, когда национальное государство может координировать свои усилия на нескольких платформах. Политики должны смотреть на эти результаты через две призмы: безопасность платформ социальных сетей и уровень контроля безопасности, который платформы предлагают политикам как конечным пользователям. Мы не рекомендуем политикам прекращать использование этих платформ, а скорее сосредоточить свои усилия на зрелых платформах с рейтингом не менее 2,7 или выше.

С макроэкономической точки зрения сами платформы социальных сетей, хотя и очень конкурентоспособны, могли бы взять пример с Центров обмена и анализа информации и более тесно обмениваться информацией, которая, вероятно, лучше контролировала бы и блокировала ботов.

NextGov: Хорошо, последний вопрос каждому из вас. Во-первых, для вас, Марк, что можно сделать, чтобы напрямую защитить машины и системы для голосования, чтобы обеспечить честность наших предстоящих выборов?

Стэмфорд: Внедрение многофакторной аутентификации для всех, кто участвует в выборах, — хорошая отправная точка. И убедитесь, что любая система голосования либо построена надежно, либо, по крайней мере, прошла некоторое тестирование, чтобы увидеть, насколько она безопасна. И не размещайте в сети ничего, чего не должно быть. Вам также необходимо обеспечить безопасность цепочки поставок систем голосования, включая аппаратное и программное обеспечение.

Наконец, постарайтесь быть двухпартийным во всем этом. В интересах обеих сторон, если мы разберемся с этим, а не спорим о том, о чем люди хотят спорить.

Nextgov: А для вас, Мэтт, что должны сделать правительство и политики, чтобы обеспечить безопасность своих учетных записей в социальных сетях, и чтобы социальные сети не могли использоваться национальными государствами или другими группами для косвенного «взлома» выборов?

Киоди: Во-первых, политики или все, кто использует социальные сети, должны убедиться, что они используют надежные пароли с помощью менеджера паролей и включают самую эффективную форму 2FA. Не используйте двухфакторную аутентификацию на основе SMS, так как ее легко использовать и она является излюбленной для злоумышленников. В Facebook и Twitter это означает

использование чего-то вроде YubiKey, чтобы воспользоваться сверхбезопасным развивающимся стандартом FIDO2. К сожалению, на таких платформах, как TikTok, используется двухфакторная аутентификация на основе электронной почты или, что еще хуже, двухфакторная аутентификация на основе SMS, которая очень восприимчива к атакам на основе SIM-карты. Во-вторых, политикам следует рассмотреть возможность обновления раздела 230 Закона о приличии в коммуникациях, чтобы обеспечить надзор за безопасностью и конфиденциальностью платформ социальных сетей, которые сейчас доминируют в политическом ландшафте США. Существует тонкий баланс между слишком слабым и слишком большим регулированием». ***(John Breeden. Both voting systems and the voters themselves could be targets of malign influence // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/experts-weigh-strengths-and-vulnerabilities-election-cybersecurity/379273/). 03.11.2022).***

***

«Сохраняйте терпение, поскольку сотрудники избирательных комиссий продолжают выполнять свою работу и проводить процесс сертификации», — сказал Истерли.

Директор Агентства кибербезопасности и безопасности инфраструктуры (CISA) Джен Истерли сделала сегодня следующее заявление о безопасности и устойчивости выборов 2022 года:

«Я хочу выразить благодарность работникам избирательных участков и сотням тысяч американцев, которые вчера служили в качестве работников избирательных участков. Работники государственных и местных избирательных комиссий уже много работали и будут продолжать делать это в ближайшие дни, чтобы подтвердить результаты выборов. Они служат на передовой нашей демократии и заслуживают нашей поддержки, восхищения и уважения. CISA с гордостью называет их партнерами. Именно благодаря им мы все можем быть уверены в безопасности, надежности и честности наших выборов.

«Мы не видели никаких доказательств того, что какая-либо система голосования удаляла или теряла голоса, изменяла голоса или каким-либо образом была скомпрометирована в какой-либо гонке в стране.

«Прямо сейчас сотрудники избирательных комиссий подсчитывают голоса, проверяют процедуры, а также тестируют и проверяют оборудование в рамках строгого процесса после дня выборов, который включает в себя завершение и сертификацию результатов. Важно помнить, что этот тщательный и совещательный процесс может занять дни или недели, в зависимости от законов штата; благодаря этим строгим процедурам американский народ может быть уверен в безопасности и честности выборов. Мы призываем всех обращаться к представителям избирательных комиссий штата и местных органов власти за самой точной и актуальной информацией о подсчете голосов и сохранять терпение, поскольку должностные лица избирательных комиссий продолжают выполнять свою работу и проводить процесс сертификации».

Являясь национальным агентством по киберзащите, Агентство по кибербезопасности и безопасности инфраструктуры возглавляет национальные

усилия по пониманию, управлению и снижению рисков для цифровой и физической инфраструктуры, на которые американцы полагаются каждый час каждого дня». ***(Brian Kime. CISA Director: No Evidence That Any Voting System Missed or Altered Votes in Midterm Elections // Homeland Security Today (https://www.hstoday.us/federal-pages/dhs/cisa-director-no-evidence-that-any-voting-system-missed-or-altered-votes-in-midterm-elections/). 09.11.2022).***

***

«Агентство пообещало оценить успех усилий крупных поставщиков программного обеспечения по включению ведения журналов и других основных функций безопасности в свои продукты «по умолчанию», но мало рассказало о том, как оно на самом деле намеревается это сделать.

Директор Агентства кибербезопасности и безопасности инфраструктуры Джен Истерли вновь обратилась к таким компаниям, как Microsoft, с призывом прекратить продавать базовые функции безопасности в качестве дополнений к своим основным продуктам.

«У нас должна быть [многофакторная аутентификация] по умолчанию. Мы не можем взимать дополнительную плату за ведение журнала безопасности и [единый вход]», — сказал Истерли. Нам нужно убедиться, что мы собираемся вместе, чтобы действительно защитить технологическую экосистему, а не возлагать бремя на тех, кто меньше всего способен защитить себя».

В беседе с Сюзанной Сполдинг из Центра стратегических и международных исследований во вторник директор CISA обсудил необходимость изменения рыночных стимулов для таких компаний, чтобы защитить критически важную инфраструктуру США от кибератак.

«Если программное обеспечение и продукты сходят с конвейера, изобилующие уязвимостями, мы никогда не решим эту проблему», — сказал Истерли, признав при этом динамичность, сформулированную Сполдингом, когда компании ускоряют разработку за счет безопасности, потому что последствия не перевешивают ущерб. преимущество в том, что они первыми продают свою продукцию.

В частности, проблема ведения журнала возникла как предмет конфликта между Microsoft и федеральными чиновниками после взлома SolarWinds, когда CISA приказала агентствам отслеживать злоумышленника в своих сетях, но поняла, что у некоторых может не быть такой возможности из-за неадекватных уровней лицензий для облачных вычислений. на базе служб Office 365…». ***(Mariam Balsh. CISA Director: Big Tech Shouldn't Charge Extra for Event Logging // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/cisa-director-big-tech-shouldnt-charge-extra-event-logging/379174/). 01.11.2022).***

***

«GAO признало усилия, уже предпринятые DOD и DIB, в результате которых количество зарегистрированных инцидентов снизилось с 3880 в 2015 году до 948 в 2021 году. Однако, несмотря на это сокращение, GAO обнаружило, что недостатки в отчетности об инцидентах остаются. Например, система отчетности

Министерства обороны обо всех инцидентах часто содержала неполную информацию, и Министерство обороны не всегда могло продемонстрировать, что оно уведомило соответствующее руководство о соответствующих критических инцидентах.

В новом отчете Счетной палаты правительства (GAO) говорится, что Министерство обороны (DOD) не полностью внедрило свои процессы для управления киберинцидентами. Государственный надзорный орган также обнаружил недостатки в отчетности и управлении данными.

Министерство обороны и военно-промышленная база США (DIB) в значительной степени зависят от информационных систем для выполнения своих операций. Эти системы по-прежнему становятся мишенью кибератак, и с 2015 года Министерство обороны США столкнулось с более чем 12 000 киберинцидентов. Например, в ноябре и декабре 2021 года китайские хакеры взломали пять оборонных и технологических компаний США. Хакеры получили пароли для доступа к системам организаций и перехвата конфиденциальных сообщений. В период с мая по июль 2019 года хакеры взломали сеть Агентства оборонных информационных систем, потенциально скомпрометировав личную информацию. Кроме того, в феврале 2017 года группа иранских хакеров нацелилась на участников, связанных с DIB, в ходе кампании по краже учетных данных и других данных.

Инциденты со злонамеренной логикой — установка программного обеспечения, разработанного и/или развернутого злоумышленниками со злонамеренными намерениями для получения доступа к ресурсам или информации без согласия или ведома пользователя — составляют подавляющее большинство сообщаемых киберинцидентов. Другие инциденты включают вторжение на корневом уровне, вторжение на уровне пользователя и отказ в обслуживании.

Для борьбы с киберугрозой Министерство обороны установило два процесса управления инцидентами: один для всех инцидентов и один для критических инцидентов. GAO признало усилия, уже предпринятые DOD и DIB, в результате которых количество зарегистрированных инцидентов снизилось с 3880 в 2015 году до 948 в 2021 году. Однако, несмотря на это сокращение, GAO обнаружило, что недостатки в отчетности об инцидентах остаются. Например, система отчетности Министерства обороны обо всех инцидентах часто содержала неполную информацию, и Министерство обороны не всегда могло продемонстрировать, что оно уведомило соответствующее руководство о соответствующих критических инцидентах.

В отчете GAO от 14 ноября отмечается, что 91% отчетов о киберинцидентах не содержат информации о дате обнаружения инцидента, что препятствует способности Министерства обороны определять, были ли сообщения об инцидентах своевременными. В отчете добавляется, что 68 процентов отчетов о киберинцидентах не включали информацию о векторе доставки инцидента, что ограничивало способность Министерства обороны выявлять тенденции распространенности различных угроз, затрагивающих его сети.

GAO объяснило недостатки в реализации двух процессов тем, что Министерство обороны, среди прочего, не назначило организацию, ответственную за обеспечение надлежащей отчетности об инцидентах и соблюдение инструкций.

Чиновники Министерства обороны признали, что его система управления инцидентами имеет ограничения, и сообщили GAO, что рассматривают возможность внедрения нового решения для устранения этих ограничений.

Обзор также показал, что Министерство обороны не полностью внедрило процесс управления критическими кибер-инцидентами из-за отсутствия подробных процедур для определения того, какие инциденты являются критическими.

Что касается кибератак на DIB, GAO обнаружило, что информация, представленная компаниями DIB в Центр киберпреступности Министерства обороны США (DC3), не всегда была полной или своевременной. Например, примерно в 20 процентах этих отчетов об инцидентах не содержалось ответа или был неясный ответ относительно того, были ли программы, платформы или системы Министерства обороны США вовлечены в инцидент. По оценкам, 21% обязательных отчетов об инцидентах, полученных DC3, указывали на то, что неизвестно, имело ли место влияние на защищенную информацию защиты. Приблизительно в 55 % отчетов об инцидентах указывалось, что исход инцидента (успешный взлом или неудачная попытка) неизвестен.

В дополнение к исключению необходимой информации, GAO обнаружило, что компании DIB часто представляли обязательные отчеты об инцидентах за пределами трехдневного окна, необходимого для отчетности. По оценкам наблюдательного органа, 51 процент кибер-инцидентов, представленных организациями DIB с 2015 по 2021 календарный год, были отправлены более чем через четыре дня после обнаружения, а 20 процентов были отправлены более чем через 20 дней после обнаружения. Чиновники DC3 заявили, что большая часть информации неизвестна в течение трехдневного окна, необходимого для отчетности, и что нереально ожидать, что компания всегда будет располагать необходимой информацией в течение этого периода времени.

Должностные лица DC3 заявили, что во время кибер-события SolarWinds несколько объектов DIB наблюдали за наличием вредоносного ПО, но не сообщали об этом, поскольку не видели выполнения вредоносного ПО или извлечения данных.

По словам официальных лиц, Министерство обороны еще не решило, следует ли сообщать о киберинцидентах DIB, обнаруженных поставщиками услуг кибербезопасности, всем соответствующим заинтересованным сторонам. GAO указало, что в руководстве Министерства обороны США говорится, что для защиты интересов национальной безопасности киберинциденты должны координироваться между организациями Министерства обороны США и внешними источниками, такими как партнеры DIB.

На прошлой неделе совместная среда обмена информацией DOD-DIB DC3 (DCISE) официально включила 1000-го добровольного партнера в программу кибербезопасности DOD DIB. Программа работает с проверенными подрядчиками, чтобы помочь предотвратить угрозы для сетей подрядчиков. Первоначально DCISE привлекла значительное количество крупных оборонных контрактных компаний, но в последнее время рост был сосредоточен на малых и средних компаниях. Оборонные компании, участвующие в программе, получают уникальные аналитические отчеты о киберугрозах, бесплатный анализ вредоносного ПО, возможности взаимодействия с государственными и отраслевыми экспертами, а

также возможности кибербезопасности как услуги от DCISE в координации с более крупным DC3 Enterprise.

Проверка GAO также изучила утечки личных данных и обнаружила, что Министерство обороны установило процесс для определения того, следует ли уведомлять людей о утечке их личной информации (PII). Этот процесс включает в себя проведение оценки рисков, в которой учитываются три фактора: характер и конфиденциальность PII, вероятность доступа к PII и ее использования, а также тип нарушения. Однако GAO обнаружило, что Министерство обороны не всегда документирует уведомления пострадавших лиц, поскольку официальные лица заявили, что уведомления часто делаются устно или по электронной почте, и никакие записи не сохраняются.

GAO дает шесть рекомендаций, в том числе о том, что Министерство обороны возлагает ответственность за обеспечение надлежащей отчетности об инцидентах, улучшает обмен информацией о кибер-инцидентах, связанной с DIB, и документирует, когда пострадавшие лица уведомляются о нарушении PII. Минобороны согласилось с рекомендациями…» ***(Kylie Bielby. GAO Tells DoD to Ensure Cyber Incidents are Properly Reported and Shared // Homeland Security Today (https://www.hstoday.us/featured/gao-tells-dod-to-ensure-cyber-incidents-are-properly-reported-and-shared/). 15.11.2022).***

***

«GAO обнаружило, что по состоянию на август 2022 года Секретная служба [США] не начала процесс внедрения для поддержки перехода на IPv6 для каких-либо своих активов или услуг.

Счетная палата правительства заявляет, что секретной службе США необходимо обновить свой план внедрения кибербезопасности с нулевым доверием. Однако в целом правительственный надзорный орган признал прогресс Секретной службы в этой области.

Архитектура нулевого доверия (ZTA) — это набор принципов кибербезопасности, согласно которым организации должны проверять все, что пытается получить доступ к их системам и службам. Принцип нулевого доверия основан на концепции, согласно которой нельзя доверять ни одному действующему лицу, действующему вне или внутри сети организации. ZTA обеспечивает комплексный мониторинг безопасности, детальный контроль доступа на основе рисков и автоматизацию системной безопасности скоординированным образом во всех аспектах инфраструктуры.

Федеральное правительство начало попытки использовать ZTA. С 2020 года Национальный институт стандартов и технологий (NIST) и Административно-бюджетное управление (OMB) дали инструкции и рекомендации федеральным агентствам по использованию ZTA. Кроме того, Агентство по кибербезопасности и безопасности инфраструктуры в 2021 году выпустило проект дорожной карты по переходу на ZTA, а Закон о разрешении на национальную оборону 2022 года предписал Министерству обороны разработать стратегию нулевого доверия и типовую архитектуру.

Секретная служба США разработала план реализации четырех этапов, предназначенных для поддержки ZTA. Основные этапы: провести самооценку ИТ-среды агентства в соответствии с федеральными указаниями; внедрить предложения облачных услуг от поставщика; достичь зрелости в регистрации событий; и перевести ИТ-инфраструктуру агентства на более совершенный интернет-протокол.

GAO обнаружило, что Secret Service завершила самооценку и добилась прогресса во внедрении облачных сервисов и достижении зрелости в регистрации событий. Кроме того, у агентства был план по внедрению более совершенного интернет-протокола, но оно не соответствовало давним требованиям OMB для общедоступных систем. По словам GAO, переходя на этот протокол, агентство может использовать дополнительные функции безопасности.

Во время аудита эффективности GAO (с октября 2021 г. по ноябрь 2022 г.) Секретная служба предпринимала дополнительные усилия, которые могли бы принять меры, указанные в стратегии нулевого доверия OMB, выпущенной в январе 2022 г. В этой стратегии излагаются действия, которые агентства должны предпринять к концу финансового года. 2024 год. Однако GAO заявило, что основные этапы плана Секретной службы не охватывают все необходимые действия OMB, поскольку Секретная служба разработала свой план реализации до того, как OMB опубликовало стратегию. Тем не менее проверка показала, что Секретная служба либо предпринимала действия, либо сообщала, что намерена выполнить действия, которые могут охватывать оставшиеся действия.

Здесь также стоит отметить, что в марте 2022 года Министерство внутренней безопасности (DHS) разработало собственный план реализации ZTA и представило его в OMB. DHS планирует продолжать развивать свой план реализации в соответствии с требованиями OMB. Например, он намерен использовать интегрированную проектную группу для включения таких компонентов, как секретная служба, в свои процессы планирования для включения ZTA в масштабах всего предприятия.

NIST утверждает, что ресурсы, приложения и службы, которые в основном основаны на облаке или в основном используются удаленными работниками, являются хорошими кандидатами для подхода ZTA. GAO обнаружило, что Secret Service приступила к реализации предложений поставщика облачных услуг и планирует продолжить их реализацию. Например, агентство интегрировало свою облачную службу аутентификации с локальными процессами аутентификации для синхронизации и управления учетными записями пользователей в своей ИТ-среде. Агентство также планирует развернуть инструменты для использования облачного решения, которое должно позволить управлять идентификацией пользователей и устройств с помощью неграфических пользовательских интерфейсов, таких как сценарии и инструменты командной строки. Кроме того, по состоянию на апрель 2022 года у Secret Service были планы по внедрению компонента от своего поставщика облачных услуг, предназначенного для поддержки шифрования данных, хранящихся в облаке.

Чтобы внедрить ZTA, агентства должны иметь точную, обширную и своевременную регистрацию событий, чтобы они могли отслеживать, просматривать и анализировать свои активы в режиме реального времени и в случае

события. GAO обнаружило, что по состоянию на август 2022 года Секретная служба еще не достигла базового уровня зрелости регистрации событий в соответствии со своими планами, хотя агентство внедрило инструмент для централизованной регистрации, мониторинга, проверки и анализа. Чиновники сослались на административные проблемы, связанные с задержкой использования инструмента, и заявили, что он, вероятно, будет введен в действие до конца года.

В соответствии с указаниями OMB и DHS, Секретная служба планирует перейти на версию 6 Интернет-протокола (IPv6), которая, помимо прочих преимуществ, дает федеральным агентствам большую уверенность в личности отправителя. Стратегия Secret Service на май 2021 года описывает этапы и прогнозируемые затраты, связанные с переводом до 80 процентов своих активов на IPv6. Однако GAO обнаружило, что по состоянию на август 2022 года Secret Service еще не начала процесс внедрения для поддержки перехода на IPv6 для каких-либо своих активов или услуг. В отчете GAO говорится, что «общедоступные почтовые серверы Секретной службы не принимали электронную почту IPv6 и не имели оперативного включения IPv6, хотя OMB потребовало от агентств сделать это к концу 2012 финансового года. В результате Секретная служба не могла принимать электронную почту через Интернет через IPv6, вынуждая внешние системы электронной почты с поддержкой IPv6 прибегать к подключению IPv4 для доставки электронной почты в Секретную службу». Кроме того, GAO обнаружило, что по состоянию на август 2022 года секретная служба не настроила восемь общедоступных систем для оперативного использования IPv6. «Из-за этого агентство не могло принимать внешние подключения IPv6 к системам, которые оно перечисляет как общедоступные», — отмечается в отчете. «Это вынудило внешних клиентов с поддержкой IPv6 вернуться к подключению IPv4 для подключения к системам».

Чиновники сообщили GAO, что ограничения не позволили агентству выделить средства на персонал и оборудование, необходимые для перевода активов на IPv6. В августе 2022 года официальные лица добавили, что они получили финансирование и находятся в процессе выделения средств для выполнения своего плана.

GAO дало секретной службе две рекомендации. Во-первых, чтобы выполнить невыполненные требования Управления управления и бюджета для перехода на IPv6, особенно в отношении модернизации своих общедоступных систем, над чем, по словам Секретной службы, они работают к 30 сентября 2025 года. И во-вторых, чтобы обновить свой план внедрения ZTA. чтобы включить все усилия, связанные с переходом на ZTA, который Секретная служба заявила, что рассчитывает сделать до конца года». ***(Kylie Bielby. GAO Checks Secret Service's Progress on Zero Trust Architecture // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/gao-checks-secret-services-progress-on-zero-trust-architecture/). 19.11.2022).***

***

«5G соединяет системы, которые позволят обрабатывать огромные объемы данных по беспроводной связи в режиме реального времени в любой точке мира.

Сегодня Центр сотрудничества по кибербезопасности Агентства национальной безопасности (АНБ) выпустил последнее видео из серии выступлений по кибербезопасности, в котором основное внимание уделяется тому, как безопасность 5G влияет на национальную безопасность. Серия выступлений представляет собой форум для АНБ, на котором они могут поделиться своими знаниями, уроками и вкладом в свою работу в области кибербезопасности.

В сегодняшнем видео технический сотрудник АНБ по кибербезопасности доктор Джозайя Дайкстра встретился с руководителем Enduring Security Framework (ESF) АНБ Натали Питторе и руководителем АНБ по разработке стандартов 5G Мартином Голдбергом.

Беспроводная технология пятого поколения (5G) представляет собой следующую эволюцию сетей мобильной связи, представляя множество новых соединений, возможностей и услуг. От автомобилей до мобильных телефонов и средств ведения боевых действий — 5G революционизирует способ общения и обмена информацией в мире.

Представьте себе миллиарды подключенных устройств, собирающих и обменивающихся информацией в режиме реального времени. 5G поддерживает такие приложения, как умные дома и здания, умные города и удаленные медицинские услуги. Технологии 5G также поддерживают массивную межмашинную связь для автоматизации отрасли. Эти новые функции и новые услуги требуют нового способа развертывания передовых мобильных услуг, а также новых подходов к совместной работе технологий 5G.

«Безопасность 5G является важнейшим компонентом национальной безопасности. В АНБ у нас есть надежная миссия по кибербезопасности, поэтому приоритетом является то, чтобы в 5G с самого начала была заложена вся безопасность», — сказал Питторе. «АНБ также является агентством боевой поддержки; наша миссия состоит в том, чтобы гарантировать, что боец сможет выполнить свою миссию с помощью надежной надежной защищенной связи».

5G — это больше, чем просто модернизация беспроводной связи; 5G соединяет системы, которые позволят обрабатывать огромные объемы данных по беспроводной сети в режиме реального времени — в любой точке мира.

«Что делает 5G действительно особенным, так это то, что это технология, позволяющая использовать другие типы продуктов, поэтому рассмотрите умные города или системы интеллектуального трафика», — сказал Голдберг. «Важность 5G заключается в том, что это не универсальный тип технологии. Раньше с 4G он был действительно разработан только для пользователя. 5G может обеспечить подключение к светофорам, где ему не нужна такая большая пропускная способность, как смартфону».

Организации по разработке стандартов (SDO) играют ключевую роль в обеспечении безопасности продуктов, предназначенных для 5G, до начала производства. Цель стандартов — прийти к соглашению о функциональности, функциях, совместимости и безопасности новых технологий. Разработка стандартов гарантирует, что решения будут доступны пользователям и разработчикам в различных секторах и экосистемах.

«Поскольку 5G становится частью приложения, вы должны доверять этому соединению, верить, что сообщение будет доставлено. Нам нужно заняться безопасностью с первого же дня и принять активное участие в органах по стандартизации, чтобы это было частью уравнения, а не чем-то постфактум», — сказал Голдберг.

Чтобы узнать больше о 5G от руководителя отдела разработки стандартов АНБ ESF и 5G, посмотрите полное видео.

Посетите канал АНБ на YouTube, чтобы увидеть все выпуски серии выступлений по кибербезопасности». ***(Cybersecurity Speaker Series: 5G Security Impacts National Security // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/cybersecurity-speaker-series-5g-security-impacts-national-security/). 22.11.2022).***

***

«Управление генерального инспектора (OIG) Департамента транспорта (DOT) инициировало проверку внедрения департаментом инструментов непрерывного мониторинга для повышения кибербезопасности.

DOT использует программные инструменты в своих сетях для защиты активов информационных технологий в рамках своей программы непрерывного мониторинга информационной безопасности. Целью программы является борьба федеральных агентств с угрозами кибербезопасности путем обнаружения рисков кибербезопасности для федеральных информационных систем и данных практически в режиме реального времени.

Крайне важно, чтобы программные инструменты DOT эффективно определяли, подвержены ли системы Департамента риску компрометации злоумышленниками, для защиты данных DOT и защиты его информационных систем и устройств. Чтобы помочь Департаменту улучшить свою позицию в области кибербезопасности и снизить риски кибербезопасности, OIG оценит инструменты непрерывного мониторинга DOT для обнаружения, предотвращения и сообщения об угрозах кибербезопасности, которые могут поставить под угрозу информационные системы и данные DOT.

Предыдущие проверки OIG выявили множество уязвимостей в области кибербезопасности в DOT, над устранением которых сейчас работает департамент». ***(OIG Initiates Cybersecurity Audit at DOT // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/transportation/oig-initiates-cybersecurity-audit-at-dot/). 22.11.2022).***

***

«Министерство обороны (DoD) опубликовало свою Стратегию нулевого доверия и дорожную карту.

Текущие и будущие киберугрозы и атаки вызывают необходимость в подходе Zero Trust (ZT), который выходит за рамки традиционного подхода к защите периметра. Министерство обороны намерено внедрить отдельные возможности и мероприятия ZT, как указано в стратегии и связанной с ней дорожной карте, к 27 ФГ.

Стратегия предусматривает, что информационное предприятие Министерства обороны защищено полностью внедренной структурой кибербезопасности ZT для всего департамента, которая уменьшит поверхность атаки, обеспечит управление рисками и эффективный обмен данными в партнерских средах, а также быстро сдержит и устранит действия злоумышленников.

В стратегии изложены четыре комплексные стратегические цели высокого уровня, которые определяют, что будет делать Департамент для реализации своего видения ZT:

Принятие культуры нулевого доверия — все сотрудники Министерства обороны осведомлены, понимают, обучены и привержены мышлению и культуре нулевого доверия и поддерживают интеграцию ZT.

Информационные системы Министерства обороны защищены и защищены. Практики кибербезопасности включают ZT в новые и устаревшие системы.

Ускорение технологий. Технологии внедряются со скоростью, равной или превышающей отраслевые достижения.

Поддержка нулевого доверия — процессы, политики и финансирование на уровне отдела и компонента синхронизированы с принципами и подходами ZT.

Внедрение нулевого доверия будет непрерывным процессом перед лицом постоянно меняющихся угроз со стороны противника и новых технологий. Дополнительные усовершенствования Zero Trust будут внесены в последующие годы по мере изменения технологий и развития противников Соединенных Штатов.

Стратегию нулевого доверия Министерства обороны и дорожную карту можно найти в библиотеке DoD CIO. ***(DoD Releases Zero Trust Strategy and Roadmap // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/dod-releases-zero-trust-strategy-and-roadmap/). 28.11.2022).***

***

«Поскольку мы рассматриваем эту новую норму цепочек поставок с новыми рисками и угрозами, необходим новый подход для обеспечения безопасности наших цепочек поставок технологий.

Специалисты по информационным системам Управления транспортного командования, управления, связи и киберсистем Томас Рём (слева) и Росс Ли (справа) добавляют программное обеспечение и создают образы новых ноутбуков 15 апреля 2020 года на базе ВВС Скотт, штат Иллинойс. Управление готовило ноутбуки для раздачи членам команды, чтобы максимально увеличить возможности удаленной работы во время пандемии COVID-19.

Двадцать лет назад наиболее частым нарушением цепочек поставок были фабричные пожары. Сегодня этот ландшафт значительно изменился. Глобализация привела к распределенным цепочкам поставок. Логистика на основе искусственного интеллекта позволяет доставлять компоненты точно в срок. Однако эффективность также породила хрупкость. В системе слишком мало резервов для обеспечения устойчивости перед лицом сбоев.

Сегодня есть несколько крупных источников сбоев. Изменение климата вызывает более экстремальные погодные явления, которые являются основным источником нарушений. COVID-19 привел к появлению новых способов и моделей

закупок, и в сочетании с нехваткой рабочей силы он продолжает сбивать с толку розничные и потребительские цепочки поставок. Растущая торговая напряженность с Китаем, вызванная стремлением к превосходству в экономической сфере и национальной безопасности, наряду с санкциями, введенными по всему Тихоокеанскому региону, продолжают нарушать цепочки поставок технологий. Наконец, новые угрозы, такие как программы-вымогатели, создают новые риски для производителей.

Поскольку мы рассматриваем эту новую норму цепочек поставок с новыми рисками и угрозами, необходим новый подход для обеспечения безопасности наших цепочек поставок технологий. Хотя основное внимание в этой статье уделяется цепочкам поставок технологий, эти принципы применимы и к более широким аспектам отказоустойчивости, а также к более широким цепочкам поставок.

1. Мы должны освещать цепочки поставок, чтобы вы могли видеть, что вы покупаете и у кого.

В то время как большинство организаций хорошо разбираются в своих прямых поставщиках, немногие знают, кто их поставщики второго уровня. Что касается программного обеспечения, инициатива Software Bill of Materials (SBOM) призвана помочь обеспечить это освещение. По мере того, как поставщики начинают требовать от своих поставщиков SBOM, мы в конечном итоге можем получить список всех программных библиотек и строительных блоков, которые входят в конечный продукт или услугу.

2. Мы должны быть в состоянии принимать решения о поставщиках с учетом рисков и угроз.

Например, программное обеспечение, основанное на неподдерживаемой библиотеке с открытым исходным кодом, может представлять риск. Точно так же продукты китайских компаний могут представлять угрозу. Закон о разрешении на национальную оборону 2023 года содержит формулировку, которая требует от Министерства внутренней безопасности покупать только программное обеспечение для критически важных функций, которое не имеет известных уязвимостей. Кроме того, Министерство торговли прямо запретило китайские товары, такие как Huawei, в определенных секторах.

3. На национальном уровне нам необходимо сформировать экосистему надежных поставщиков, инвестируя в американских и смежных производителей.

Недавно принятый законопроект «ЧИПС+Наука» включает ассигнования в размере 54 миллиардов долларов на поддержку отечественного производства беспроводных устройств и полупроводников. Что касается беспроводной связи, Национальное управление по телекоммуникациям и информации выделит гранты в размере 1,5 миллиарда долларов американским компаниям для восстановления американской производственной экосистемы телекоммуникаций, которая атрофировалась за последние 20 лет и была продана по частям в Европу. Для полупроводников массивные субсидии помогут восстановить развитие полупроводников в США.

4. Мы должны инвестировать в американские инновации, чтобы следующая волна технологий уже находилась в США и не нуждалась в офшорах.

Американские университеты и промышленность должны возглавлять НИОКР и соединять эти технологии с долиной смерти, поэтому новые научные и технологические инновации накапливаются в ВВП США. Научная часть законопроекта «CHIPS + Science» включает в себя новые разрешения на сотни миллиардов долларов для научных агентств США, таких как Министерство энергетики, Национальное управление по аэронавтике и исследованию космического пространства, Национальный институт стандартов и технологий и Национальный научный фонд. Надеюсь, Конгресс выделит необходимые ассигнования для активизации этих амбиций.

5. Нам нужно перейти в наступление.

Как мы видим на примере санкций против России, можно подвергнуть риску всю национальную экономику, систематически ограничивая цепочки поставок. Более целенаправленные эффекты могут быть достигнуты за счет более узкого манипулирования конкретными элементами цепочки поставок. Если злоумышленники вмешиваются в цепочки поставок США, мы должны пресечь их.

Мы находимся в уникальном моменте времени. Мы сталкиваемся с новыми рисками и угрозами. На горизонте у нас большие инвестиции в новые федеральные технологии. Понимая взаимосвязь, мы можем создать более безопасную технологическую цепочку поставок, которая справляется с этими новыми рисками и угрозами». ***(Charles Clancy. Five Principles to Help Secure Technology Supply Chains // Homeland Security Today (https://www.hstoday.us/featured/five-principles-to-help-secure-technology-supply-chains/). 29.11.2022).***

***

«Голова Твіттера Ілон Маск прийняв на роботу хакера Джорджа Хотца, який став відомим завдяки зламу ігрової приставки Sony PlayStation 3 та випуску джейлбрейка для iPhone. Наразі Хотц проходитиме 12-тижневий випробувальний термін, після якого Маск вирішить його подальшу долю у компанії.

Перед відомим хакером поставлено 2 основних завдання: вирішити проблеми з пошуковою системою Twitter та прибрати вікно авторизації, яке блокує доступ до пошуковика незареєстрованим користувачам. Джордж Хотц виявив бажання працювати в Twitter після того як Ілон Маск звільнив 75% співробітників — з 7500 до 2750 осіб. За словами Хотца, його зацікавив рішучий підхід Маска до роботи та його безкомпромісні рішення.

Цікаво, що це не перша спроба хакера працювати в компанії Ілона Маска — ще у 2015 році Хотц обговорював можливість своєї роботи в Tesla над проектами, пов’язаними з технологіями автономного управління рухом авто. Втім, тоді Джордж відмовився від угоди, публічно заявивши, що «роботу він насправді не шукав», і пообіцявши знову зв’язатися з Маском, «коли зламає систему Mobileye».

Щодо Твіттера, враховуючи масштаб звільнень, співробітники, які залишились, очікують, що платформа скоро почне ламатися. Команда, яка підтримує базові системні бібліотеки Twitter, якими користується кожен інженер компанії, також пішла. «Ви не можете керувати Twitter без цієї команди», — сказав співробітник, що звільняється.

Нова чистка рядів Twitter відбулася одразу після того, як Маск звільнив десятки співробітників, які критикували або висміювали його у твітах та внутрішніх повідомленнях. Потім Маск встановив крайній термін о 17:00 у четвер, щоб усі співробітники відповіли «так» у формі Google, якщо вони хочуть залишитися в тому, що він називає «Twitter 2.0».

Згідно з концепцією Twitter 2.0, компанія працюватиме над шифруванням повідомлень і додасть можливість надсилання зашифрованих відео та здійснення голосових дзвінків. «Ми хочемо, щоб користувачі могли спілкуватися, не турбуючись про свою конфіденційність та викрадення їх даних з Twitter. Ми хочемо, щоб користувачі припинили думати, що хтось у Твіттері може шпигувати за ними», — наголосив Ілон Маск». ***(Ілон Маск найняв хакера, щоб він відремонтував Twitter // Internetua (https://internetua.com/ilon-mask-nainyav-hakera-sxob-vin-vidremontuvav-twitter). 24.11.2022).***

***

«Чиновники кибербезопасности США говорят, что не было никаких доказательств значительного вмешательства со стороны хакерских групп, поскольку опросы по всей стране открыты для промежуточных выборов. Утром в день выборов высокопоставленный сотрудник Агентства кибербезопасности и безопасности инфраструктуры сообщил журналистам, что они «по-прежнему не видят конкретной или реальной угрозы нарушения избирательной инфраструктуры», сообщает CNN.

Представитель CISA заявил, что агентство ожидает возможных низкоуровневых кибератак, которые могут временно сделать недоступными государственные и местные веб-сайты, но не предвидит каких-либо проблем, которые помешали бы гражданам проголосовать.

«Мы по-прежнему сохраняем высокую уверенность в безопасности или устойчивости выборов», — заявил чиновник.

Киберкомандование США и Агентство национальной безопасности обмениваются оперативными обновлениями с другими правительственными учреждениями, чтобы обеспечить промежуточную защиту от потенциальных внешних угроз, согласно заявлению во вторник генерала, курирующего обе операции.

«Мы продолжаем уточнять то, что узнали на выборах 2018 и 2020 годов», — сказал генерал Пол Накасоне. «Мы генерируем понимание, чтобы обеспечить защиту родины, и, в конечном итоге, накладываем расходы, унижая и разоблачая возможности и операции иностранного противника».

Накасоне также подтвердил, что сотрудники разведки также сосредоточены на кампаниях иностранного влияния, которые продолжаются после подсчета голосов после дня выборов.

«Наша работа не заканчивается 8 ноября», — сказал Накасоне.

Представитель министерства обороны заявил, что двенадцать штатов задействовали отряды Национальной гвардии для киберподдержки на местных выборах и выборах на уровне штатов». ***(THEARA COLEMAN. No signs of significant hacking issues on Election Day, cyber security officials say // Future US LLC***

(https://theweek.com/stephen-colbert/1018301/stephen-colberts-late-show-had-a-soundtrack-for-election-night-then-an-80s). 08.11.2022).

***

«После громких инцидентов кибербезопасности за последние несколько лет, включая атаки SolarWinds, Log4j и Colonial Pipeline в 2021 году, правительство США издало директивы и рекомендации по обеспечению кибербезопасности в цифровой экосистеме и на протяжении всего жизненного цикла. Белый дом и федеральные агентства стремились укрепить кибербезопасность как правительства, так и отрасли, сохраняя при этом нашу наиболее важную инфраструктуру в безопасности, отказоустойчивости и работоспособности.

В нескольких администрациях Конгресс принял законодательство и финансирование ключевых программ и возможностей кибербезопасности. Промышленность продолжает инвестировать и совершенствовать инструменты кибербезопасности и меры по смягчению последствий. Эти шаги свидетельствуют о взрослении коллективной национальной киберзащиты и подчеркивают необходимость продолжения сотрудничества между отраслью и правительством.

Акцент на безопасность и отказоустойчивость инфраструктуры

В апреле 2021 года Министерство энергетики (DOE) запустило государственно-частную инициативу по повышению кибербезопасности систем промышленного контроля электроэнергетических компаний, а Белый дом продолжил ряд дополнительных отраслевых программ, в том числе программу для водного сектора, а также недавно объявленная государственно-частная инициатива по кибербезопасности в химическом секторе.

Администрация транспортной безопасности (TSA) также приняла отраслевой подход. После атаки программы-вымогателя Colonial Pipeline агентство координировало свои действия с заинтересованными сторонами в отрасли и межведомственными партнерами для разработки ряда директив по безопасности для поддержки критически важных результатов кибербезопасности для операторов трубопроводов. TSA также выпустило пару директив для пассажирских и грузовых железнодорожных перевозчиков, которые включали требования по применению защитных мер для раннего смягчения угроз кибербезопасности.

Этой осенью Федеральная комиссия по регулированию энергетики объявила о своем намерении разработать правила поощрения тарифов на добровольные инвестиции коммунальных предприятий в кибербезопасность, включая показатели эффективности кибербезопасности. Аналогичным образом, Министерство энергетики опубликовало свою Национальную стратегию киберинженерии, в которой содержится призыв к повышению прозрачности киберугроз в энергетических системах.

Киберриск как бизнес-риск и императив национальной безопасности

Ранее в этом году Комиссия по ценным бумагам и биржам США обратилась к сообщениям о киберинцидентах и опыту совета директоров в области кибербезопасности в предложенных правилах. Когда Национальный институт стандартов и технологий приступил к запланированному обновлению своей основополагающей концепции кибербезопасности (CSF), заместитель министра

торговли Дон Грейвс определил управление рисками кибербезопасности как часть ведения бизнеса, назвав его критически важным для экономической безопасности нашей страны.

Федеральное правительство также использует мощь кошелька, чтобы снизить киберриски и повысить безопасность цифровой экосистемы. В сентябре Административно-бюджетное управление выпустило руководство для федеральных агентств, требующее от них использовать программное обеспечение, созданное с использованием методов безопасного программного обеспечения. А в прошлом месяце Агентство по кибербезопасности и безопасности инфраструктуры (CISA) выпустило последнюю из серии обязательных операционных директив. Это требует от агентств улучшить видимость активов и обнаружение уязвимостей, а также сообщать эту информацию через федеральную панель непрерывной диагностики и смягчения последствий CISA.

Обмен информацией и сотрудничество в отрасли

В марте президент Байден подписал Закон об отчетности о кибер-инцидентах в отношении критически важной инфраструктуры от 2022 года (CIRCIA). Законодательство предоставит правительству, владельцам и операторам инфраструктуры, а также другим заинтересованным сторонам лучшее представление о постоянно меняющемся ландшафте киберугроз. Примечательно, что язык CIRCIA подчеркивает роль как правительства, так и промышленности. Он требует, чтобы организации предоставляли CISA информацию об определенных типах инцидентов кибербезопасности и платежей программ-вымогателей, а также требует, чтобы CISA возвращала ценную информацию.

В прошлом месяце CISA также опубликовала Цели эффективности кибербезопасности (CPG). Добровольные межсекторальные цели устанавливают общий набор основных методов кибербезопасности для критической инфраструктуры, согласованных с существующими структурами, включая NIST CSF.

CPG являются началом межотраслевых переговоров между отраслью и правительством о том, как наилучшим образом управлять факторами киберриска, уникальными для каждого сектора, а также понимать и сообщать о безопасности и экономических затратах на инвестиции в безопасность. В CPG и других недавних руководствах подчеркивается острая необходимость укрепления доверия и прозрачности в государственном и частном секторах, включая как владельцев-операторов инфраструктуры, так и сообщество поставщиков.

Согласованный национальный инвестиционный подход

Предыдущие директивы, относящиеся к ранним дням существования Министерства внутренней безопасности, определяли национальную политику по поддержанию устойчивой критически важной инфраструктуры и закладывали основу для текущего сотрудничества между отраслью и правительством. Эти нынешние действия подтверждают безопасность инфраструктуры как национальную безопасность.

Недавние инциденты, затрагивающие заинтересованные стороны далеко за пределами целевых организаций, подчеркивают настоятельную необходимость для владельцев и операторов государственной инфраструктуры (включая федеральных,

государственных, местных, племенных и территориальных), а также сообществ поставщиков и поставщиков технологий сотрудничать для обеспечения безопасности цифровой экосистемы.

Энн Нойбергер, заместитель советника Белого дома по национальной безопасности по кибербезопасности и новым технологиям, недавно описала «неустанное внимание» к защите важнейших секторов инфраструктуры, чтобы помочь им улучшить свою кибербезопасность. Предварительно представляя предстоящую национальную стратегию кибербезопасности, национальный директор по кибербезопасности Крис Инглис указал, что его офис будет использовать как рыночные силы, так и регуляторные и политические рычаги для привлечения инвестиций в кибербезопасность, подчеркивая, что киберриск является бизнес-риском и риском для национальной безопасности.

Комиссия по солярию киберпространства США также подчеркнула важность киберустойчивой инфраструктуры как для национальной, так и для экономической безопасности, призвав к формальному планированию, в консультации с частным сектором, для обеспечения непрерывности экономики и непрерывной работы критически важных функций в случае крупного кибер инцидент.

В конечном счете, инвестиционные решения принимаются на организационном уровне, но имеют гораздо более широкие последствия. Это особенно верно в отношении взаимозависимой системы отраслей, жизненно важные функции которых опираются на общую инфраструктуру. Когда правительство использует политику для поощрения и обеспечения принятия правильных решений об инвестициях в киберриски, эти инвестиции приносят каскадные выгоды для нашей коллективной безопасности.

Чтобы получить измеримые результаты в области кибербезопасности в масштабе, национальный подход должен основываться на действиях и инвестициях.

Крайне важно предоставить правительству информацию, необходимую для формирования эффективной политики; обеспечить, чтобы отрасль могла принимать инвестиционные решения с учетом рисков, и поощрять максимально тесное сотрудничество государственного и частного секторов. Основа политики, созданная за последние несколько лет и в ближайшие годы, проложит путь для более активных действий и инвестиций в соответствии с национальными и организационными приоритетами кибербезопасности». ***(Katherine D. Ledesma. Why the public and private sectors must join forces to address cyber risk for national security // NEXSTAR MEDIA INC. (https://thehill.com/opinion/cybersecurity/3750096-why-the-public-and-private-sectors-must-join-forces-to-address-cyber-risk-for-national-security/). 25.11.2022).***

***

Країни ЄС та Великобританія

«Европейская комиссия и Верховный представитель представили Совместное сообщение о политике ЕС в области киберзащиты и План действий по военной мобильности 2.0 для решения проблемы ухудшения условий

безопасности после агрессии России против Украины и повышения способности ЕС защищать своих граждан и инфраструктуру.

Благодаря своей новой политике в области киберзащиты ЕС расширит сотрудничество и инвестиции в киберзащиту, чтобы лучше защищать, обнаруживать, сдерживать и защищать от растущего числа кибератак.

Полный пресс-релиз:

Сегодня Комиссия и Высокий представитель представили Совместное сообщение о политике ЕС в области киберзащиты и План действий по военной мобильности 2.0 для решения проблемы ухудшения условий безопасности после агрессии России против Украины и повышения способности ЕС защищать своих граждан и инфраструктуру.

Благодаря своей новой политике в области киберзащиты ЕС расширит сотрудничество и инвестиции в киберзащиту, чтобы лучше защищать, обнаруживать, сдерживать и защищать от растущего числа кибератак.

Киберпространство не имеет границ. Недавние кибератаки на энергетические сети, транспортную инфраструктуру и космические объекты показывают риски, которые они представляют как для гражданских, так и для военных субъектов. Это требует дополнительных действий для защиты граждан, вооруженных сил, а также гражданских и военных миссий и операций ЕС от киберугроз.

Политика ЕС в отношении киберзащиты направлена на расширение возможностей киберзащиты ЕС и укрепление координации и сотрудничества между военными и гражданскими киберсообществами (гражданскими, правоохранительными, дипломатическими и оборонными). Это повысит эффективность управления киберкризисами в ЕС и поможет уменьшить нашу стратегическую зависимость от критических кибертехнологий, а также укрепить Европейскую оборонно-технологическую промышленную базу (EDTIB). Это также будет стимулировать обучение, привлечение и удержание кибер-талантов и активизировать сотрудничество с нашими партнерами в области киберзащиты.

Политика ЕС в отношении киберзащиты построена вокруг четырех столпов, которые охватывают широкий спектр инициатив, которые помогут ЕС и государствам-членам:

Действовать вместе для усиления киберзащиты ЕС: ЕС укрепит свои механизмы координации между национальными и европейскими игроками в области киберзащиты, чтобы увеличить обмен информацией и сотрудничество между военными и гражданскими сообществами кибербезопасности, а также и далее поддерживать военные миссии и операции CSDP.

Защитите оборонную экосистему ЕС: даже некритические программные компоненты могут использоваться для проведения кибератак на компании или правительства, в том числе в оборонном секторе. Это требует дальнейшей работы по стандартизации и сертификации кибербезопасности для защиты как военных, так и гражданских доменов.

Инвестировать в возможности киберзащиты: Государства-члены должны совместно значительно увеличить инвестиции в современные военные средства киберзащиты, используя платформы сотрудничества и механизмы финансирования,

доступные на уровне ЕС, такие как PESCO, Европейский оборонный фонд, а также Horizon Европа и программа «Цифровая Европа».

Партнер для решения общих проблем: опираясь на существующую безопасность и оборону, а также кибердиалоги со странами-партнерами, ЕС будет стремиться к установлению индивидуальных партнерских отношений в области киберзащиты.

Следующие шаги

Комиссия и Высокий представитель, в том числе в его качестве главы Европейского оборонного агентства (EDA), будут представлять ежегодный отчет Совету ЕС для мониторинга и оценки хода реализации действий, предусмотренных Совместным сообщением о Политика ЕС по киберзащите. Государствам-членам предлагается вносить свой вклад в ход реализации мер по реализации, осуществляемых в национальных форматах или в формате сотрудничества. План реализации может быть разработан в сотрудничестве с государствами-членами.

Фон

В Стратегии кибербезопасности ЕС на 2020 год подчеркивается необходимость пересмотра основ политики ЕС в области киберзащиты. Кроме того, в своем обращении к Конгрессу в 2021 году президент фон дер Ляйен призвала к разработке Европейской политики киберзащиты. Это также является целью Стратегического компаса по безопасности и обороне, утвержденного Советом в марте этого года. В мае в выводах Совета о развитии киберпозиции Европейского Союза государства-члены предложили Высокому представителю вместе с Комиссией представить амбициозное предложение по Политике киберзащиты ЕС в 2022 году.

Вместе с пакетом «Безопасность и оборона» Комиссия также публикует сегодня первый отчет о ходе выполнения Плана действий по синергии между гражданскими, оборонными и космическими отраслями, доступный здесь». ***(Cyber Defence: EU boosts action against cyber threats // Shaping Europe's digital future (https://digital-strategy.ec.europa.eu/en/news/cyber-defence-eu-boosts-action-against-cyber-threats). 10.11.2022).***

***

«Эта онлайн-сессия Connect University будет посвящена Закону о киберустойчивости и тому, как он защищает экономику Европы и нашу коллективную безопасность, и в то же время повышает осведомленность европейских потребителей о кибербезопасности.

Предложение Комиссии о новом Законе о киберустойчивости (CRA), объявленное президентом Урсулой фон дер Ляйен в сентябре 2021 года во время ее обращения к нации в Европейском союзе и основанное на Стратегии кибербезопасности ЕС на 2020 год и Стратегии Союза безопасности ЕС на 2020 год, обеспечит что цифровые продукты, такие как беспроводные и проводные продукты и программное обеспечение, более безопасны для потребителей в ЕС: помимо повышения ответственности производителей, обязывая их предоставлять поддержку безопасности и обновления программного обеспечения для устранения выявленных

уязвимостей, это позволит потребителям иметь достаточную информацию о кибербезопасности продуктов, которые они покупают и используют.

2/3 кибератак связаны с уязвимостями, 60% продуктов, размещаемых на рынке, содержат известные уязвимости. В соответствии с законом неадекватные функции безопасности останутся в прошлом с введением обязательных требований кибербезопасности для производителей и розничных продавцов таких продуктов, причем эта защита будет распространяться на весь жизненный цикл продукта.

Оратор:

Киркетерп де Вирон Кристиан, руководитель отдела политики кибербезопасности и цифровой конфиденциальности, DG Connect, Европейская комиссия». ***(Cyber Resilience Act: new EU cybersecurity rules ensure safer hardware and software // Shaping Europe's digital future (https://digital-strategy.ec.europa.eu/en/events/cyber-resilience-act-new-eu-cybersecurity-rules-ensure-safer-hardware-and-software). 22.11.2022).***

***

«Старшие представители по кибербезопасности государств-членов ЕС, Агентства ЕС по кибербезопасности (ENISA) и Комиссии приняли участие в двухдневных учениях Blueprint Operational Level, или Blue OLEx 2022, для проверки процедур антикризисного управления.

В свете предстоящего внедрения Директивы о сетях и информационных системах (NIS2) крупномасштабные учения по кибербезопасности помогли улучшить общую координацию, осведомленность о ситуации и процесс принятия решений, а также способствовали укреплению доверия и обмену информацией, в том числе между государствами-членами. и Комиссия.

Тьерри Бретон, комиссар по внутреннему рынку, сказал:

Больше, чем когда-либо, мы видим, как злоумышленники разрабатывают новые стратегии, нацеленные на нашу цифровую инфраструктуру и услуги, подвергая риску граждан и компании. Кибератаки происходят повсюду, и мы несем общую ответственность за совместную работу по подготовке и реализации планов быстрого реагирования на чрезвычайные ситуации, особенно в случае крупномасштабного киберинцидента или кризиса.

Вслед за Blue OLEx 2021 в этом году учения были организованы властями Литвы при поддержке ENISA в рамках Европейской сети организаций по связям с кибер-кризисами, или «EU-CyCLOne». EU-CyCLOne поддерживает скоординированное управление крупномасштабными инцидентами и кризисами в области кибербезопасности и обеспечивает регулярный обмен информацией между государствами-членами и институтами, органами и агентствами Союза. Он способствует реализации плана Европейской комиссии для быстрого экстренного реагирования в случае крупномасштабного трансграничного киберинцидента путем обеспечения сотрудничества между техническим (например, Группой реагирования на инциденты компьютерной безопасности — CSIRT) и политическим уровнями (например, Интегрированное реагирование на политические кризисы — IPCR) при крупномасштабном — имеет место масштабный трансграничный киберкризис». ***(Commission and EU countries simulate large-scale cyber-attacks to foster preparedness***

// Shaping Europe's digital future (https://digital-strategy.ec.europa.eu/en/news/commission-and-eu-countries-simulate-large-scale-cyber-attacks-foster-preparedness). 07.11.2022).

***

«Европейский совет принял закон о высоком общем уровне кибербезопасности на территории Союза с целью дальнейшего повышения устойчивости и потенциала реагирования на инциденты как государственного, так и частного секторов, а также ЕС в целом. Новая директива под названием «NIS2» заменит действующую директиву по безопасности сетей и информационных систем (директива NIS).

«Нет никаких сомнений в том, что кибербезопасность останется ключевой проблемой в ближайшие годы. Ставки для нашей экономики и наших граждан огромны. Сегодня мы сделали еще один шаг, чтобы улучшить нашу способность противостоять этой угрозе», — сказал Иван Бартош, вице-премьер Чехии по цифровизации и министр регионального развития.

Более эффективное управление рисками и инцидентами и сотрудничество

NIS2 установит базовый уровень для мер по управлению рисками кибербезопасности и обязательств по отчетности во всех секторах, на которые распространяется действие директивы, таких как энергетика, транспорт, здравоохранение и цифровая инфраструктура.

Пересмотренная директива направлена на гармонизацию требований кибербезопасности и реализацию мер кибербезопасности в разных государствах-членах. Для этого он устанавливает минимальные правила для нормативно-правовой базы и устанавливает механизмы для эффективного сотрудничества между соответствующими органами в каждом государстве-члене. Он обновляет список секторов и видов деятельности, на которые распространяются обязательства по кибербезопасности, и предусматривает средства правовой защиты и санкции для обеспечения соблюдения.

Директива официально учредит Европейскую сеть организации по связи с киберкризисами, EU-CyCLONe, которая будет поддерживать скоординированное управление крупномасштабными инцидентами и кризисами в области кибербезопасности.

Расширение сферы действия правил

В то время как в старой директиве NIS государства-члены несли ответственность за определение того, какие организации будут соответствовать критериям, чтобы квалифицироваться как операторы основных услуг, новая директива NIS2 вводит правило предельного размера в качестве общего правила для идентификации регулируемых организаций. Это означает, что все средние и крупные предприятия, работающие в секторах или предоставляющие услуги, подпадающие под действие директивы, подпадают под ее действие.

Хотя пересмотренная директива сохраняет это общее правило, ее текст включает дополнительные положения, обеспечивающие пропорциональность, более высокий уровень управления рисками и четкие критерии критичности, позволяющие

национальным органам определять дополнительные объекты, на которые распространяется действие.

В тексте также уточняется, что директива не будет применяться к организациям, осуществляющим деятельность в таких областях, как оборона или национальная безопасность, общественная безопасность и правоохранительные органы. Судебная система, парламенты и центральные банки также исключены из сферы действия.

NIS2 также будет применяться к государственным администрациям на центральном и региональном уровнях. Кроме того, государства-члены могут решить, что это применимо и к таким организациям на местном уровне.

Другие изменения, внесенные новым законом

Кроме того, новая директива была приведена в соответствие с отраслевым законодательством, в частности с положением о цифровой операционной устойчивости для финансового сектора (DORA) и директивой об устойчивости критически важных объектов (CER), чтобы обеспечить юридическую ясность и согласованность между NIS2 и эти акты.

Добровольный механизм взаимного обучения повысит взаимное доверие и позволит изучить передовую практику и опыт Союза, тем самым способствуя достижению высокого общего уровня кибербезопасности.

Новое законодательство также упорядочивает обязательства по предоставлению отчетности, чтобы избежать чрезмерного предоставления отчетности и создания чрезмерного бремени для охватываемых организаций.

Следующие шаги

Принятие Советом ЕС происходит через несколько недель после того, как Европейский парламент одобрил новый закон.

Директива NIS2 будет опубликована в Официальном журнале Европейского союза в ближайшие дни и вступит в силу в середине декабря.

У государств-членов будет 21 месяц с момента вступления директивы в силу, чтобы включить ее положения в свое национальное законодательство. (Хотя следует отметить, что еще есть некоторые государства-члены ЕС, которые еще не внедрили меры, предусмотренные Директивой NIS.)». ***(EU Council adopts the NIS2 directive // Help Net Security (https://www.helpnetsecurity.com/2022/11/29/eu-council-adopts-the-nis2-directive/). 29.11.2022).***

***

«Национальный центр кибербезопасности Соединенного Королевства (NCSC) недавно опубликовал свой Ежегодный обзор за 2022 год, в котором сообщается о состоянии угроз кибербезопасности в стране. Как технический орган Великобритании по кибербезопасности, NCSC выпускает ежегодный отчет, охватывающий киберугрозы за предыдущие 12 месяцев, а также анализ потенциальных будущих проблем.

В отчете NCSC говорится, что программы-вымогатели остаются постоянной угрозой как для бизнеса, так и для государственных служб в Великобритании. В течение отчетного периода с сентября 2021 г. по август 2022 г. NCSC отмечает, что в Великобритании было совершено 18 атак программ-вымогателей, которые

требовали скоординированного ответа на национальном уровне. Это включало нападения на поставщика NHS 111, службы экстренной медицинской помощи, а также на компанию South Staffordshire Water, занимающуюся водоснабжением и коммунальными услугами.

Не приводя конкретных инцидентов, NCSC также выражает озабоченность по поводу угроз международной кибербезопасности, исходящих как от России, так и от Китая. В течение отчетного периода Россия стремилась использовать подрывные кибероперации для поддержки своей военной кампании во время вторжения в Украину, а NCSC помогал украинским властям в их киберзащите. Несмотря на выдающиеся усилия России, как отмечает NCSC, техническая эволюция Китая, вероятно, станет единственным крупнейшим фактором, влияющим на состояние кибербезопасности Великобритании в будущем. NCSC отмечает, что деятельность Китая стала более изощренной, и страна все чаще ориентируется на сторонние технологии и цепочки поставок услуг, а также использует уязвимости программного обеспечения.

NCSC прогнозирует, что распространение и коммерческая доступность кибервозможностей будут продолжаться, а новые вредоносные киберинструменты станут доступными для более широкого круга государственных и негосударственных субъектов. Кроме того, NCSC считает, что эти инструменты будут применяться чаще и с меньшей предсказуемостью, что увеличит угрозу для Великобритании. Таким образом, NCSC «усилил» свою автоматизированную службу уведомлений, запустив службу, которая предупреждает участников о потенциальных угрозах, рисках, уязвимостях или открытых портах в их сетях. NCSC подробно описывает различные другие действия, которые он предпринял, чтобы помочь предприятиям и государственному сектору повысить устойчивость и реагирование на киберугрозы, включая участие сообщества и расширение объема рекомендаций и руководств, выпущенных NCSC». ***(Kim Peretti, Kristen Bartolotta. UK's National Cyber Security Centre Releases 2022 Annual Review // Alston & Bird (https://www.alstonprivacy.com/uks-national-cyber-security-centre-releases-2022-annual-review/?cn-reloaded=1). 07.11.2022).***

***

«Национальное агентство кибербезопасности и информационной безопасности сообщает, что количество киберинцидентов в Чехии в прошлом месяце было намного выше среднего, достигнув самого высокого уровня с апреля.

В заявлении, опубликованном во вторник, официальные лица говорят, что в октябре они зафиксировали 19 кибератак, некоторые из которых были совершены группой «Анонимная Россия».

Почти 70 процентов зарегистрированных инцидентов были DDoS-атаками.

В прошлом месяце также произошел первый с мая инцидент, классифицированный как «очень значительный». Это касалось телекоммуникационных услуг». ***(High number of cyber-attacks recorded in October, says security agency // Radio Prague International (https://english.radio.cz/high-number-cyber-attacks-recorded-october-says-security-agency-8766476). 08.11.2022).***

***

«Согласно шестому ежегодному обзору отрасли, проведенному Jisc, кибербезопасность остается приоритетной задачей для высших руководителей британских колледжей, университетов и исследовательских центров.

Тем не менее, д-р Джон Чепмен, директор Jisc по политике и управлению информационной безопасностью, который проводит ежегодное исследование, предупреждает, что среда угроз остается сложной, и самоуспокоенности быть не может.

Опрос, проведенный в июне 2022 года и получивший 123 ответа от британских учреждений, показывает, что почти все 97% высших учебных заведений и 94% поставщиков дополнительного образования включают кибербезопасность в свой реестр рисков, что на два и пять процентных пунктов больше, чем в сравнении. до 2021 года.

Многие также регулярно сообщают о киберрисках и устойчивости своему исполнительному совету; 87% организаций ВО и 79% организаций ИП…

Оценка кибербезопасности

Статистика также свидетельствует о том, что создание сильной системы кибербезопасности остается сложной задачей. На вопрос: « Насколько хорошо, по вашему мнению, защищена ваша организация?» ', организации высшего образования проявляют осторожность: только 16% (10 из 62 учреждений) набрали восемь или более баллов (где 10 – лучшая защита).

Восприятие более позитивно в FE, 39% оценивают свою организацию как восемь и более.

Комментарии к этому вопросу предполагают, что организации, оценивающие себя от пяти до семи, имеют средства контроля, но понимают, что всегда нужно сделать больше, чтобы не отставать от угроз.

Для тех, кто набрал от восьми до десяти баллов, ключевыми темами были важность надежных систем и процессов, наряду с аудитами, сертификацией и внешней поддержкой…

Основные угрозы

Программа-вымогатель/вредоносное ПО названа в опросе главной угрозой для организаций высшего образования (HE), а фишинг/социальная инженерия – угрозой номер один для дополнительного образования (FE). Неисправленные уязвимости занимают третье место как для HE, так и для FE.

Обязательный инструктаж по вопросам безопасности чаще проводится для сотрудников, чем для студентов: его проводят 84 % организаций высшего образования и 77 % организаций FE. Как и в предыдущие годы, организации ДО (21%) чаще проводят обязательное обучение студентов, чем ВО (5%)…» ***(Results of cyber security survey of UK colleges and universities // FE News (https://www.fenews.co.uk/education/results-of-cyber-security-survey-of-uk-colleges-and-universities/). 08.11.2022).***

***

«Коммунальные предприятия представляют собой часть критической национальной инфраструктуры в Великобритании и подвержены киберугрозам даже в мирное время, когда враги — и, хотите верьте, хотите нет друзья — постоянно выгрызают слабые места в сети, чтобы определить устойчивость и потенциальные дыры.

Однако коммунальные предприятия могут смягчить эти угрозы, чтобы гарантировать, что коммерческая деятельность не будет скомпрометирована.

На этом цифровом поле битвы ведется бесчисленное множество способов — от нарушения работы корпоративных систем, лежащих в основе коммерческих и человеческих операций коммунальной компании, до более злонамеренного вмешательства операционных технологий, призванного нанести серьезный ущерб гражданскому обществу.

Атака вредоносного ПО AcidRain в феврале этого года привела к серьезному и длительному нарушению работы в массовом масштабе. Атака уничтожила спутниковые модемы широкополосного сервиса KA-SAT коммуникационной компании Viasat, затронув тысячи людей в Украине и других странах Европы.

Наводнение 1997 года в Великобритании привело к полной потере снабжения чистой водой в ряде регионов, а в прошлом году кибератака вынудила оператора Colonial Pipeline временно закрыть 8 851 км (5 500 миль) трубопровода. Более того, враждебное вмешательство в Украине привело к отключению энергетики — в данном случае ветровых электростанций.

В конечном счете, в эпоху Интернета вещей (IoT), когда машины в доме, в торговле и во всей промышленности получают идентификацию и возможность общаться, этот риск только возрастет.

Противодействие угрозе

По данным IBM, энергетическая отрасль заняла пятое место по общим затратам на утечку данных в 2021 году, а безопасность в секторе коммунальных услуг требует дополнительных соображений: это строго регулируемая отрасль, где утечка информации может быть чрезмерно дорогостоящей по стандартам любой другой отрасли. Более того, расходы, связанные с программами-вымогателями или кибератаками, могут быстро возрасти. В период с 2020 по 2021 год сообщалось о 10-процентном увеличении с 3,86 млн долларов США (3,37 млн фунтов стерлингов) до 4,24 млн долларов США (3,7 млн фунтов стерлингов) за каждый инцидент с утечкой данных. Кроме того, есть время, необходимое для обнаружения нарушения; часто чем дольше нарушение остается незамеченным, тем дороже и/или разрушительнее инцидент. И, наконец, штрафы, налагаемые контролирующими органами. И все это до того, как мы перейдем к репутационному ущербу.

Кибербезопасность уже является приоритетом для многих коммунальных предприятий, и, к счастью, существует множество способов противодействия этим угрозам, начиная с признания этой присущей уязвимости и внедряя культуру осведомленности, которая формирует более безопасное поведение, процессы и дизайн системы.

Защита сетей

Риск возрастает, когда или если данные подвергаются открытому Интернету, поэтому коммунальные предприятия должны использовать контроль, используя

новейшие IP-технологии — безопасно работая в общедоступных сетях или работая через безопасные частные сети. Частные сети и выделенные концентраторы, например, в спутниковой системе TSAT, поддерживают жизненно важный воздушный зазор между телеметрией и управлением, а также открытыми общедоступными сетями. С другой стороны, корпоративные системы часто маршрутизируются через интернет-протоколы, они по своей природе более заметны и, следовательно, уязвимы. В идеале данные SCADA и телеметрии не будут смешиваться с корпоративным трафиком. Безопасное разделение помогает гарантировать, что эти данные не попадут в чужие руки.

Здесь и сейчас

По мере того как изо дня в день Интернет вещей все больше внедряется в промышленность, становится жизненно важным, чтобы все устройства и локальные сети, связанные с сетью, содержали технологии и программное обеспечение для их защиты.

Одним из таких способов является технология SD WAN (программно определяемая, WAN), которая защищает данные от внешнего мира. Эта технология также обеспечивает стабильную производительность и отказоустойчивость приложений за счет автоматического управления трафиком в зависимости от приложений на основе бизнес-целей, протоколов безопасности и архитектуры глобальной сети.

Одним из преимуществ данных телеметрии является их относительный размер. Поскольку для данных телеметрии требуется меньшая полоса пропускания, чем для большей части трафика, проходящего через корпоративную систему, их может быть труднее отследить. Хотя первичным каналам и платформам потребуются альтернативы и резервные копии, что означает решения для спутников, LTE, 4g/5g.

В нашей недавней статье «Путь компании Data в формировании цифровой трансформации в сфере коммунальных услуг и что все это означает» мы исследуем, как данные стали катализатором цифровизации среди компаний в секторе коммунальных услуг, и как сбои и перебои в поставках приводят к огромному финансовому бремени и штрафам для поставщика и серьезные (часто продолжительные) сбои для потребителей.

Что возвращает нас к началу: осознание рисков, в том числе признание того, что они могут исходить из более близкого дома, чем может показаться на первый взгляд, так же важно, как и данные, которые необходимо защитить». ***(Alastair MacLeod. Cyber security: Why the utilities sector must mitigate threats from outside and within // EMAP PUBLISHING LIMITED (https://www.newcivilengineer.com/latest/cyber-security-why-the-utilities-sector-must-mitigate-threats-from-outside-and-within-08-11-2022/). 08.11.2022).***

***

«Сегодня Комиссия и Высокий представитель представили Совместное сообщение о политике ЕС в области киберзащиты и План действий по военной мобильности 2.0 для решения проблемы ухудшения условий безопасности после агрессии России против Украины и повышения способности ЕС защищать

своих граждан и инфраструктуру. Благодаря своей новой политике в области киберзащиты ЕС расширит сотрудничество и инвестиции в киберзащиту, чтобы лучше защищать, обнаруживать, сдерживать и защищать от растущего числа кибератак. Киберпространство не имеет границ. Недавние кибератаки на энергетические сети, транспортную инфраструктуру и космические объекты показывают риски, которые они представляют как для гражданских, так и для военных субъектов. Это требует дополнительных действий для защиты граждан, вооруженных сил, а также гражданских и военных миссий и операций ЕС от киберугроз. Политика ЕС в отношении киберзащиты направлена на расширение возможностей киберзащиты ЕС и укрепление координации и сотрудничества между военными и гражданскими киберсообществами (гражданскими, правоохранительными, дипломатическими и оборонными). Это повысит эффективность управления киберкризисами в ЕС и поможет уменьшить нашу стратегическую зависимость от критических кибертехнологий, а также укрепить Европейскую оборонно-технологическую промышленную базу (EDTIB). Это также будет стимулировать обучение, привлечение и удержание кибер-талантов и активизировать сотрудничество с нашими партнерами в области киберзащиты.

Политика ЕС в отношении киберзащиты построена вокруг четырех столпов, которые охватывают широкий спектр инициатив, которые помогут ЕС и государствам-членам:

Действовать вместе для усиления киберзащиты ЕС: ЕС укрепит свои механизмы координации между национальными и европейскими игроками в области киберзащиты, чтобы расширить обмен информацией и сотрудничество между военными и гражданскими сообществами кибербезопасности, а также и далее поддерживать военные миссии и операции в рамках ОПБО.

Защитите оборонную экосистему ЕС: даже некритические программные компоненты могут использоваться для проведения кибератак на компании или правительства, в том числе в оборонном секторе. Это требует дальнейшей работы по стандартизации и сертификации кибербезопасности для защиты как военных, так и гражданских доменов.

Инвестировать в средства киберзащиты: государствам-членам необходимо совместно значительно увеличить инвестиции в современные военные средства киберзащиты, используя платформы сотрудничества и механизмы финансирования, доступные на уровне ЕС, такие как PESCO, Европейский оборонный фонд, а также Horizon. Европа и программа «Цифровая Европа».

Партнер для решения общих проблем: опираясь на существующую безопасность и оборону, а также кибердиалоги со странами-партнерами, ЕС будет стремиться к установлению индивидуальных партнерских отношений в области киберзащиты.

Следующие шаги

Комиссия и Высокий представитель, в том числе в его качестве главы Европейского оборонного агентства (EDA), будут представлять ежегодный отчет Совету ЕС для мониторинга и оценки хода реализации действий, предусмотренных Совместным сообщением о Политика ЕС по киберзащите. Государствам-членам предлагается вносить свой вклад в ход реализации мер по реализации,

осуществляемых в национальных форматах или в формате сотрудничества. План реализации может быть разработан в сотрудничестве с государствами-членами.

В Стратегии кибербезопасности ЕС на 2020 год подчеркивается необходимость пересмотра основ политики ЕС в области киберзащиты. Кроме того, президент фон дер Ляйен призвала к разработке Европейской политики киберзащиты в своем обращении к Конгрессу в 2021 году. Это также является целью Стратегического компаса по безопасности и обороне, утвержденного Советом в марте этого года. В мае в выводах Совета о развитии киберпозиции Европейского Союза государства-члены предложили Высокому представителю вместе с Комиссией представить амбициозное предложение по Политике киберзащиты ЕС в 2022 году…» ***(Cyber Defence: EU boosts action against cyber threats // European Commission (https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6642). 10.11.2022).***

***

«Усиление кибератак на правительственные структуры и органы госуправления, рост хактивизма, а также продуцирование и распространение дезинформации с использованием искусственного интеллекта (ИИ) и дипфейков — эти киберугрозы существенно возросли с момента начала войны в Украине. Их результат — все более широкомасштабные атаки, имеющие все более разрушительные последствия.

Об этом говорится в опубликованном в четверг ежегодном докладе Европейского агентства по кибербезопасности (ENISA). В документе, озаглавленном Threat Landscape 2022 (ETL) анализируется период с июля 2021 года по июль 2022 года.

По мнению ENISA, геополитическая ситуация, и в первую очередь война в Украине, изменили положение дел в глобальной киберсфере. 24% всех кибератак были направлены на органы государственного управления и правительственные структуры, а также на основные сектора экономики — энергетику, транспорт, банковское дело и цифровую инфраструктуру.

13% всех осуществленных кибератак были направлены против поставщиков цифровых услуг.

«Сегодняшний глобальный контекст неизбежно вызывает серьезные изменения в ландшафте угроз кибербезопасности. Новая парадигма формируется растущим кругом участников угроз. Мы вступаем в фазу, когда потребуются соответствующие стратегии смягчения последствий для защиты всех наших важнейших секторов, наших отраслевых партнеров и, следовательно, всех граждан ЕС», — заявил в четверг исполнительный директор ENISA Юхан Лепассаар.

В докладе также отмечается, что ежемесячно в ЕС крадется более 10 терабайт данных, программы-вымогатели по-прежнему считаются одной из основных угроз, а фишинг теперь определяется как наиболее распространенный начальный вектор подобных атак. Среди программ-вымогателей первое место занимают атаки на доступность, также называемые атаками распределенного отказа в обслуживании (DDoS). По данным ENISA, от 60% организаций, пострадавших от программ-вымогателей, могли потребовать выкуп.

DDoS-атаки становятся все более масштабными и сложными, перемещаясь в мобильные сети и Интернет вещей (IoT), которые сейчас используются в кибервойне.

Первичные киберугрозы были проанализированы с точки зрения их мотивации. В отчете ENISA подчеркивается, что хакеры, спонсируемые государствами, мотивированы геополитическими целями, такими как шпионаж и саботаж. Кибероперации хактивистов мотивируются идеологическими целями.

ENISA отмечает угрозы распространения дезинформации и дипфейков с помощью ИИ. Увеличивается количество ботов, моделирующих реальных персонажей, что может легко нарушить процесс нормотворчества в органах управления стран ЕС, наводнив сайты правительственных учреждений поддельным контентом и комментариями…» ***(Европейское агентство по кибербезопасности: война в Украине изменила спектр киберугроз // Голос Америки (https://www.golosameriki.com/a/europe-cyber-threats/6818417.html). 03.11.2022).***

***

«С надвигающейся рецессией в Великобритании предприятия сталкиваются с перспективой сокращения в нескольких областях, чтобы обеспечить выживание. Ничего не решено, и, к сожалению, это также может означать сокращение бюджетов на кибербезопасность.

В условиях роста затрат и усилий по контролю счетов за электроэнергию компаниям, возможно, придется проявлять творческий подход и искать способы экономии в таких областях, как расходы на облачные вычисления и даже на кибербезопасность. Последнее, однако, может показаться опасной перспективой, учитывая растущий спектр киберугроз, таких как программы- вымогатели.

По данным OpenText Security, две трети (67%) малых и средних предприятий (SMB) тратят менее 50 000 долларов в год на кибербезопасность, при этом 57% опасаются, что инфляция приведет к изменению планов, что приведет к сокращению бюджета.

Это беспокойство возникает, несмотря на недавний всплеск кибератак, что подчеркивает необходимость надлежащего финансирования стратегии кибербезопасности. На самом деле, это ставит очень уместный вопрос о том, как организации могут поддерживать тот же уровень защиты, стремясь урезать бюджеты.

Основные принципы снижения затрат

К бюджетам кибербезопасности нельзя относиться легкомысленно; необходимо иметь несколько руководящих принципов для обеспечения соблюдения основных стандартов при снижении рисков.

Технический директор Global Rubrik MSP Assured Data Protection Стью Паркин рассказал ИТ -специалистам, что он стал свидетелем того, как клиенты начали задумываться об уменьшении дублирования функций и функций, включенных в продукты, которые они покупают.

«Компании часто спешат на рынок, чтобы купить как можно больше, чтобы заполнить определенный пробел», — говорит он. «Однако эти пробелы теперь могут быть заполнены одним или сокращенным списком поставщиков или продуктов.

Экономическая эффективность часто достигается за счет объединения лицензий, а также за счет объединения навыков внутренних команд и центров управления безопасностью (SOC)».

Однако Ли МакМаллен, выдающийся вице-президент по аналитике исследовательской фирмы Gartner, говорит, что он не видит снижения затрат, и основная задача директора по информационной безопасности и группы кибербезопасности состоит в том, чтобы защитить ценностное предложение предприятия. «До сих пор это была игра, в которой возможны только нулевые баллы — вы не страдаете от инцидента — или отрицательный — вы получаете», — говорит МакМаллен. «Вместо этого ведущие мыслители уделяют гораздо больше внимания устойчивости. Хотя ни один CISO не может предложить «идеальную защиту», они могут предложить повышенный уровень устойчивости и возможности восстановления ценностного предложения».

Первые шаги к сокращению бюджетов на кибербезопасность

Одним из первых приоритетов для бизнеса при сокращении расходов на кибербезопасность является попытка понять объем систем и активов, которые бизнес пытается защитить. Затем следует оценка уровня риска для этих систем, говорит Мартин Уолшем, директор по кибербезопасности в консалтинговой компании по кибербезопасности AMR CyberSecurity.

«Когда у бизнеса есть понимание этого, тогда у него есть хорошая возможность рассмотреть приоритеты с точки зрения бюджета и усилий для управления самыми высокими уровнями риска в своей организации», — говорит он.

Он добавляет, что есть несколько ключевых соображений относительно того, когда бизнес должен также оценить, где и как он тратит бюджет, чтобы убедиться, что он расходуется разумно. Есть ряд вопросов, представляющих собой своего рода контрольный список, которые предприятия должны задавать себе, в основном охватывающих самые основы.

По словам Уолшема, тратить большие суммы денег на современные инструменты, такие как программное обеспечение для кибербезопасности на основе ИИ, например, не имеет смысла, если организация не устанавливает исправления и не контролирует свою конфигурацию. Компании также должны спросить себя, возможно ли встроить безопасность в контракты на аутсорсинговые услуги. «Это позволяет избежать дополнительных внутренних затрат и обеспечивает надлежащее управление контрактами со сторонними организациями», — говорит он.

Еще один вопрос, который следует учитывать, заключается в том, представляют ли услуги и инструменты, которые использует организация, соотношение цены и качества. Уолшем говорит, что это может показаться простым, но удивительно, как много организаций не могут правильно оценить.

Между тем, по словам Брайана Мартина, руководителя отдела продуктов, стратегии и инноваций в консалтинговой компании по кибербезопасности Integrity360, также важно сравнение с хорошо работающими аналогами. «Мы знаем, что бенчмаркинг имеет решающее значение для успешного распределения бюджета безопасности. Таким образом, после того, как все сделано правильно и проанализировано, директора по информационной безопасности могут затем

вернуться и начать решать, где они могут позволить себе сократить расходы, имея полную картину», — говорит он.

На каких затратах на кибербезопасность можно сэкономить?

Сокращение расходов на кибербезопасность может стать возможностью упростить ситуацию. По словам Майка Фрая, директора практики безопасности MSP Maintel в Великобритании и Ирландии, со временем структура безопасности организации может превратиться в сложную сеть разрозненных продуктов. Каждый из этих продуктов будет иметь свою стоимость, поставщиков и накладные расходы на управление ИТ.

«Применяя стратегический подход и работая с ключевыми поставщиками с широкими возможностями, это можно рационализировать для повышения эффективности, снижения нагрузки на ИТ и сокращения затрат», — говорит он. «В некоторых случаях предприятия могут сократить свои расходы до 50%».

Мартин добавляет, что, к сожалению, нельзя назвать определенную цифру возможной экономии, поскольку она просто зависит от отправной точки для каждой конкретной организации, их стратегии и склонности к риску.

«Однако хорошо известно, например, что покупка службы SOC или службы управляемого обнаружения и реагирования (MDR) может стоить вдвое меньше, чем ее создание и укомплектование персоналом собственными силами», — возражает он. «Переговоры с поставщиками, комплектация и долгосрочные контракты часто могут обеспечить ежегодную экономию более 10%».

Не экономьте на общей защите

Предприятия должны правильно понять основы и повысить свою устойчивость на 360 градусов. Организациям рекомендуется избегать подхода «заприте дверь и оставьте окно открытым», который ставит под угрозу базовую инфраструктуру безопасности и объединяет организационные потребности, говорит Нехал Такоре, глава UKI в Bosch CyberCompare.

«Чтобы создать целостную стратегию кибербезопасности, предприятия могут внедрить структуру Национального института стандартов и технологий (NIST), — говорит Такоре. Он добавляет, что основанная на пяти ключевых принципах — идентификация, защита, обнаружение, реагирование и восстановление — структура NIST помогает предприятиям любого размера лучше понимать, управлять и снижать риски кибербезопасности, обеспечивая при этом защиту сетей и данных.

«Компании могут лучше решать, в какие области лучше всего инвестировать время и деньги в защиту кибербезопасности», — продолжает Такоре. «Регулярные меры по повышению осведомленности о кибербезопасности и обучение сотрудников являются важным способом обеспечения общей защиты».

Мартин добавляет, что для обеспечения общей защиты крайне важен разумный баланс инвестиций в участие человека и автоматизацию. «Это должно быть подкреплено очень четкой стратегией безопасности и соответствием структуре безопасности, которая будет давать рекомендации относительно того, какие основные элементы управления не могут быть скомпрометированы». ***(Rene Millman. How to reduce cyber security costs for your business // Future Publishing Limited (https://www.itpro.co.uk/security/369523/how-to-reduce-cyber-security-costs-for-your-business). 16.11.2022).***

***

«Нидерланды — одна из самых цифровизированных стран мира. Голландцы все чаще работают, живут, делают покупки и встречаются в цифровом пространстве, что делает цифровые системы бьющимся сердцем общества. Это предлагает множество возможностей, но также и риски, поскольку безопасность в цифровом мире отстает от безопасности в физическом мире.

Теперь правительство Нидерландов разработало новую национальную стратегию кибербезопасности, направленную на обеспечение цифровой защиты голландского общества. Киберугрозы существуют постоянно и их количество растет, а преступники и государственные деятели угрожают организациям всех типов.

Вот почему правительство Нидерландов принимает меры для повышения цифровой устойчивости страны, укрепления систем безопасности и устранения угроз. Это единственный способ безопасно получить экономические и социальные выгоды от цифровизации, защищая население, предприятия и услуги.

Большинство современных цифровых систем не были разработаны с учетом принципа безопасности. Конечные пользователи, такие как граждане, малые предприятия и крупные организации, десятилетиями несут ответственность за собственную цифровую безопасность. Но только некоторые из этих пользователей способны выполнить эту обязанность. Некоторые едва ли знают, как обновить маршрутизатор Wi-Fi, и изо всех сил пытаются защитить свои ИТ-системы или соблюдать законы о конфиденциальности.

Тем временем киберугрозы возрастают. И хотя цифровая безопасность может быть более зрелой в крупных организациях, безопасность их систем часто сводится к поведению их сотрудников. Серьезный простой находится всего в одном щелчке мыши сотрудника.

Правительство Нидерландов стремится к ситуации, при которой каждый участник цифровой экосистемы вносит свой вклад в безопасность и стабильность всей системы. Это требует коллективной трансформации, поскольку ни одна организация не может сделать это в одиночку, даже правительство. Это должны быть совместные усилия организаций, создающих цифровую инфраструктуру страны, тех, кто ею управляет, и тех, кто ее использует. Ответственность за безопасность будет переложена с конечных пользователей на правительство и секторы.

Новая стратегия кибербезопасности описывает видение правительства Нидерландов, согласно которому граждане и предприятия могут в полной мере пользоваться преимуществами цифрового общества, не беспокоясь о киберрисках. Стратегия была разработана при широком участии государственных, частных и общественных организаций.

Для реализации этого видения цели были сформулированы по четырем «столпам». Первый компонент отвечает за цифровую устойчивость правительства, бизнеса и организаций гражданского общества. Это включает в себя снижение риска до приемлемого уровня за счет набора мер по предотвращению киберинцидентов и, в случае возникновения киберинцидентов, по их обнаружению, уменьшению ущерба и упрощению восстановления.

Для этого система цифровой безопасности Нидерландов укрепляется. Например, Национальный центр кибербезопасности, Центр цифрового доверия и Группа реагирования на инциденты кибербезопасности для поставщиков цифровых услуг будут объединены в единый национальный орган кибербезопасности. Также необходимо больше информации об угрозах, потому что это единственный способ повысить устойчивость.

Второй компонент ориентирован на поставщиков и покупателей цифровых продуктов и услуг, а также на обогащение знаний и инноваций. Движение к безопасной и инновационной цифровой экономике будет способствовать цифровой безопасности Нидерландов и их способности зарабатывать.

На данный момент еще не существует комплексной системы европейского законодательства и регулирования, включая стандарты безопасности цифровых продуктов, процессов и услуг. В ближайшие месяцы Нидерланды представят в Европейском союзе аргументы в пользу согласованной системы европейских законов и правил, чтобы покупатели и потребители могли рассчитывать на более безопасные продукты и услуги.

Кроме того, необходимо постоянно укреплять знания и навыки Нидерландов в области цифровой безопасности для противодействия киберугрозам как сейчас, так и в будущем. Постоянное поддержание уровня внутренних знаний снижает зависимость от иностранных компаний, людей и технологий и открывает экономические возможности для голландского бизнеса.

Третий столп посвящен национальному и международному подходу к злоумышленникам — повышению видимости цифровой угрозы. Правительство Нидерландов несет особую ответственность и обладает инструментами для борьбы с цифровой угрозой.

Но это требует более пристального внимания к этим угрозам. Речь идет не только о лучшем наблюдении за действиями государственных и негосударственных акторов в цифровом пространстве. Политическое, дипломатическое, военное и экономическое поведение третьих стран также дает представление об их взглядах и намерениях в отношении использования цифрового пространства для достижения геополитического влияния. Чтобы способствовать общему пониманию угрозы, правительство Нидерландов будет чаще обмениваться киберразведкой, что позволит другим повысить свою устойчивость.

Четвертый компонент стратегии ориентирован на людей, стоящих за технологиями, и на цифровую устойчивость граждан. Общество играет жизненно важную роль в развитии цифровых навыков, от базовых знаний и навыков до высокого уровня знаний и специальных навыков кибербезопасности.

Чтобы предложить гражданам лучшую защиту от цифровых угроз, важно сделать голландцев более подкованными в области ИКТ и с помощью кампаний по повышению осведомленности предупредить их о действиях, которые они могут предпринять, чтобы повысить цифровую безопасность. Крайне важно иметь низкопороговый доступ к специализированной информации и советам в знакомых местах для повышения навыков цифровой безопасности.

В настоящее время цифровые навыки не являются частью образования в Нидерландах. Это нужно изменить. Цифровые навыки, направленные на

безопасность, должны быть не только включены в национальную учебную программу, но и учителя должны овладеть ими. Правительство Нидерландов признает важность предоставления школам соответствующей поддержки.

По мнению правительства Нидерландов, кибербезопасность — это инвестиции в будущее. Национальная стратегия кибербезопасности на 2022–2028 годы формирует основу для будущего, в котором несоответствие между цифровыми угрозами и цифровой устойчивостью будет и останется минимальным.

Поэтому правительство инвестирует в укрепление и трансформацию цифровой экосистемы, где отдельное лицо или организация больше не могут быть самым слабым звеном. Для реализации этой цели может потребоваться несколько сроков правления, а некоторые элементы могут даже стать постоянными целями». ***(Kim Loohuis. Dutch national cyber security strategy aims to protect digital society // TechTarget (https://www.computerweekly.com/news/252527557/Dutch-national-cyber-security-strategy-aims-to-protect-digital-society). 23.11.2022).***

***

«Премьер-министр Эстонии Кая Каллас заявила в своем вступительном слове на ежегодной национальной конференции по кибербезопасности в среду, что функционирование всего мира, с которым мы знакомы, от здравоохранения до энергетики, связано с кибербезопасностью и для того, чтобы чувствовать себя в безопасности, всегда нужно быть готовым даже к самому худшему из возможных сценариев.

Премьер-министр поблагодарил всех эстонских специалистов, которые ежедневно заботятся о безопасности нашего киберпространства.

«15 лет назад Эстония подверглась крупномасштабным кибератакам. Это открыло глаза многим странам на необходимость уделять внимание и кибербезопасности. Наряду с обычной войной России когда-то была гибридная война против Украины и других стран. снова сделал это значение особенно ясным, — сказала Каллас.

Премьер-министр подчеркнул, что противники всегда ищут слабые места, чтобы нас ранить.

«Мы должны быть готовы, и для этого мы должны продумать и отработать все наихудшие сценарии. Мы сильнее, когда мы готовы», — сказала Каллас.

Она также рассказала о важности обмена информацией в обеспечении кибербезопасности: мы должны быть прозрачными, обмениваться информацией с партнерами и не допускать ситуации, когда при разговоре о киберинцидентах слышна только версия противника о происходящем.

«Когда информацией делятся темные силы, светлые силы тоже должны это делать», — сказала она.

Премьер-министр отметил, что, говоря о кибербезопасности, нельзя забывать о человеке. Мы можем строить сильные системы, но если человек не является самым сильным звеном в цепи, реальная угроза всегда может исходить именно от него. Каллас добавила, что основой для того, чтобы смотреть в будущее, является надежная связь — мы должны убедиться, что наши связи связаны с партнерами, с которыми мы также разделяем общие ценности.

Для обеспечения устойчивости и кибербезопасности цифрового государства из государственного бюджета на следующие четыре года предусмотрено дополнительно 42 миллиона евро в год». ***(Estonian PM: Cyber security ensured by readiness for worst-case scenarios // The Baltic Times (https://www.baltictimes.com/estonian_pm__cyber_security_ensured_by_readiness_for_worst-case_scenarios/). 23.11.2022).***

***

Австралія та Нова Зеландія

«…Выступая на выставке кибербезопасности правительства Нового Южного Уэльса в 2022 году, министр по обслуживанию клиентов и цифровому правительству Виктор Доминелло объявил об 11 новых спонсорских грантах на сумму 15 000 долларов США для женщин в правительстве Нового Южного Уэльса, чтобы повысить их навыки в области кибербезопасности, и о том, что кибербезопасность Нового Южного Уэльса будет спонсировать сеть австралийских женщин в безопасности. некоммерческая организация, занимающаяся поддержкой и увеличением числа женщин в сфере безопасности.

«Эти инициативы призваны увеличить количество женщин, занимающихся кибербезопасностью, и помочь расширить навыки получателей, будь то в технических, политических, управленческих или разведывательных областях отрасли», — сказал г-н Доминелло.

«Благодаря этим инвестициям мы можем повысить квалификацию нашей рабочей силы и предложить новые интересные возможности, о которых наши кандидаты могли не подумать в прошлом.

«Несмотря на то, что Cyber Security NSW является одним из ведущих агентств в авангарде участия женщин в отрасли, как и сама кибербезопасность, эта работа не ставится и не забывается».

Министр по делам женщин Бронни Тейлор заявила, что правительство Нового Южного Уэльса меняет курс и расширяет участие женщин в отраслях, в которых традиционно доминируют мужчины.

«Правительство Нового Южного Уэльса стремится понять проблемы, с которыми сталкиваются женщины, пытаясь добиться успеха в новых высокодоходных отраслях, таких как кибербезопасность», — сказала г-жа Тейлор.

«Мы знаем, что когда женщины и девушки чувствуют себя комфортно и желанными в отрасли, они остаются в ней, поэтому так важны инициативы, которые поддерживают и поощряют женщин в осуществлении их мечты.

«Мое послание всем женщинам, рассматривающим будущее в области кибербезопасности, заключается в том, что вы нам нужны, мы ценим вас, и ваш вклад в эту сферу имеет решающее значение».

Главный директор по кибербезопасности Нового Южного Уэльса Тони Чепмен сказал, что Австралийская сеть женщин в сфере безопасности (AWSN) является идеальной организацией для спонсорства кибербезопасности Нового Южного Уэльса.

«Целью AWSN является увеличение числа женщин, поступающих на работу в австралийскую индустрию безопасности, работающих в ней и возглавляющих ее, что, в свою очередь, вдохновляет женщин на карьеру в сфере безопасности и помогает создать австралийский поток талантливых специалистов по безопасности», — сказал г-н Чепмен.

«Стратегия кибербезопасности штата Новый Южный Уэльс прогнозирует, что к 2026 году потребуется почти 17 000 новых рабочих мест в области кибербезопасности». ***(New initiatives to increase female participation in NSW Cyber Security // New South Wales (https://www.nsw.gov.au/media-releases/new-initiatives-to-increase-female-participation-nsw-cyber-security). 03.11.2022).***

***

«Австралийский центр кибербезопасности (ACSC) опубликовал свой ежегодный отчет о киберугрозах за период с июля 2021 года по июнь 2022 года.

Хотя он не включает кибератаки Optus и Medibank Private в сентябре и октябре 2022 года, в отчете содержится всеобъемлющий анализ киберпреступлений, программ-вымогателей и атак на критически важную инфраструктуру.

В отчете отмечается, что в 2021–2022 годах киберпреступления, направленные против физических лиц, такие как компрометация онлайн-банкинга и покупок, оставались одними из наиболее распространенных, в то время как компрометация деловой электронной почты (BEC) имела тенденцию к совершению крупных транзакций, таких как расчеты с недвижимостью.

В отчете рекомендуются средства защиты для отдельных лиц и организаций, а также план действий против программ-вымогателей.

Безопасность данных является фундаментальной обязанностью предприятий, которые получают личную информацию клиентов, особенно конфиденциальную информацию о состоянии здоровья. Они должны знать, какую личную информацию они хранят, где она хранится и кто имеет к ней доступ.

План реагирования на утечку данных требует, чтобы эксперты по безопасности информационных технологий расследовали причину и закрыли утечку.

Руководство должно иметь оперативную и честную связь с клиентами из группы риска, затронутыми третьими лицами, регулирующими органами и полицией.

Существуют потенциально серьезные финансовые и репутационные последствия для организаций, которые теряют недовольных клиентов, пока совет директоров и руководство расследуют кибератаку, объясняют неспособность обеспечить безопасность и защиту данных клиентов и восстанавливают нормальный бизнес.

Для публичных компаний также существует риск групповых исков инвесторов в результате снижения стоимости акций, в то время как рыночные факторы включают затраты на восстановление прав клиентов, возможные выплаты выкупа и нормативные санкции…» ***(David Jacobson. Australian Cyber Security Centre Annual Cyber Threat Report // LexBlog, Inc. (https://www.lexblog.com/2022/11/07/australian-cyber-security-centre-annual-cyber-threat-report/). 07.11.2022).***

***

«Малые предприятия продолжают относиться к кибербезопасности как к второстепенной задаче. Исследование, проведенное Банком Новой Зеландии, показало, что 53 % малых и средних предприятий заявили, что обучение кибербезопасности не является для них приоритетным направлением, в то время как только 31 % заявили об этом. Пандемия увеличила зависимость от технологий, и поведение потребителей резко изменилось. Интернет-бизнес и электронная коммерция — это будущее, и если малый бизнес хочет добиться успеха, ему необходимо инвестировать в правильные технологии и средства защиты.

Исследование показало, что 47% предприятий стали жертвами мошенников в прошлом году. Это рекордное количество инцидентов кибербезопасности, что только подчеркивает очевидную необходимость того, чтобы предприятия сохраняли бдительность. По данным правительственной группы реагирования на компьютерные чрезвычайные ситуации (CERT NZ), в 2022 году киберинциденты причинили предприятиям финансовые убытки в размере 3,7 миллиона долларов. Малые предприятия только начали вставать на ноги в постпандемическом мире, и они уже страдают от нехватки рабочей силы и навыков и завалены инфляцией и проблемами с цепочками поставок по всем фронтам. Нарушения кибербезопасности — это еще одна проблема, с которой им приходится сталкиваться, и они только добавляют нагрузки на их перегруженные плечи.

Г-н Скотт де Местре, руководитель отдела безопасности и инфраструктуры компании Employsure, ведущих австралийских специалистов по трудовым отношениям и охране труда и технике безопасности, прокомментировал: «В малом и среднем бизнесе наблюдается вопиющая нехватка знаний, когда речь идет о кибербезопасности. Работодатели часто думают, что ИТ-специалисты будут заниматься кибербезопасностью, но это две совершенно разные задачи и роли. Многие кибератаки осуществляются не опытными хакерами, их осуществляют люди, обладающие базовыми знаниями о том, насколько слабым может быть бизнес».

Г-н де Местре также добавил: «Владельцы малого бизнеса могут предпринять шаги для защиты своих данных и данных своих клиентов. Во-первых, поймите кибербезопасность. Владельцы бизнеса не должны игнорировать кибербезопасность. Они должны иметь базовое представление о том, что это влечет за собой, насколько сильны их системы и какие политики или процедуры необходимо внедрить. Национальный центр кибербезопасности (NCSC) содержит множество ценной информации, предназначенной для малого и среднего бизнеса, которая помогает понять основы. Во-вторых, наймите опытных специалистов. Некоторые вещи лучше оставить экспертам, и владельцы бизнеса должны понимать, что им нужно делегировать некоторые задачи обученным и квалифицированным специалистам. Наем экспертов по кибербезопасности может быть эффективным способом защиты бизнеса. И самое главное, обучать своих сотрудников. Работодатели могут обучать своих сотрудников осведомленности о кибербезопасности и помогать им понимать свои обязанности. Видео, статьи и

семинары — вот некоторые способы, с помощью которых владельцы бизнеса могут обучать своих сотрудников основам».

Только 6% киви-компаний имеют адекватную защиту от киберугроз. В Новой Зеландии высокая концентрация использования смартфонов, что делает бизнес более уязвимым. 90% новозеландских компаний относятся к малому бизнесу, и они считают кибербезопасность дорогими и ненужными расходами. Это заблуждение необходимо исправить, и малый бизнес должен знать, что профилактика гораздо более рентабельна и требует меньше стресса, чем необходимость реагировать на утечку данных.

Сейчас, как никогда раньше, компаниям необходимо проявлять бдительность в отношении защиты своих данных. Нарушение кибербезопасности приводит к подрыву доверия, увеличивает бизнес-риск, напрямую влияет на потерю доходов и наносит ущерб репутации; все, что малый бизнес не может себе позволить». ***(Cyber Security Attacks A Wake-up Call For Small Businesses // Scoop Media (https://www.scoop.co.nz/stories/BU2211/S00125/cyber-security-attacks-a-wake-up-call-for-small-businesses.htm). 08.11.2022).***

***

«Стратегии Австралии в области кибербезопасности выступают за ответ «всего общества» на противодействие угрозам иностранного вмешательства, но эксперты в области политики говорят, что усилия по привлечению общественности в значительной степени символичны.

Исследователи из Университета Флиндерса опросили 1500 австралийцев и провели углубленные фокус-группы в трех штатах в конце 2020 года, чтобы оценить отношение общества к институциональному доверию, цифровой грамотности и восприятию киберугроз.

Результаты исследования, опубликованные в Defense Studies, подчеркивают разрыв между политической риторикой и действиями. Авторы характеризуют реакцию Австралии как «нисходящую», «технократическую» и «управляемую элитой».

Согласно исследованию, отношение и участие граждан являются ключом к устойчивости перед лицом киберугроз, учитывая, что иностранное вмешательство часто направлено на то, чтобы подорвать доверие к демократии, манипулировать общественным мнением, посеять недоверие и подчеркнуть глубинные разногласия в обществе.

Иностранное вмешательство с помощью кибербезопасности может проявляться во многих формах, включая дезинформацию, взлом, доксинг, атаки программ-вымогателей, троллинг и использование ботов.

Соавтор, доцент Роберт Мануоринг, говорит: «Обычно мало значимых стратегических усилий по вовлечению граждан в ответные меры под руководством правительства, упуская из виду то, что часто называют «социальным слоем» кибербезопасности».

Исследование показывает, что политический подход Австралии в значительной степени рассматривает общественность как пассивную, а не как заинтересованную и уполномоченную бороться с киберугрозами.

В документе выделяются ключевые области, в которых общественное отношение к демократии, институтам и киберугрозам является потенциальной пищей для иностранных игроков.

Ответы на опросы показывают, что австралийцы не верят в добросовестность и честность государственных чиновников, их влияние на формирование политики, прозрачность и подотчетность.

Например, около 80% респондентов считают, что государственные чиновники, не использующие служебное положение для личной выгоды, являются фундаментальной чертой демократии, но только 39% считают, что эта практика поддерживается в Австралии.

Кроме того, в то время как органы государственной службы и службы безопасности полиции и вооруженных сил пользуются высоким уровнем доверия, подавляющее большинство респондентов согласны с тем, что учреждения Австралии не имеют связи с обычными людьми и управляются «большими интересами».

В документе говорится, что такое разочарование созрело для эксплуатации и может затруднить реакцию государства на киберугрозы.

Результаты опроса также показывают, что австралийские граждане не уверены в своей способности идентифицировать ложную и неверную информацию в Интернете, и только 20% «очень уверены» в своих собственных навыках медийной и цифровой грамотности.

Исследователи заключают, что киберзащита Австралии будет подкреплена более сильным вниманием к пониманию опасений и рассказов граждан…» ***(Petra Stock. Australia's approach to cyber security lacks citizen engagement // COSMOS (https://cosmosmagazine.com/australia/cyber-security-citizen-engagement/). 23.11.2022).***

***

Російська Федерація та країни ЄАЕС

«Исследование Positive Technologies показало, что IT-системы почти всех крупных российских компаний уязвимы для хакерской атаки. В 96% случаев злоумышленник мог бы преодолеть сетевой периметр и проникнуть во внутреннюю сеть.

Пентесты прошли в нескольких десятках российских компаний из различных секторов экономики, в том числе финансового, промышленного, госсектора, торгового, транспортного и других, сообщают «Ведомости».

Больше половины (57%) компаний, в которых проводилось исследование, состоят в рейтинге крупнейших компаний России по объему реализации продукции RAEX-600.

Что показало исследование:

96% компаний не защищены от проникновения внешнего злоумышленника;

в 90% случаев злоумышленник мог бы получить доступ к конфиденциальной информации, в том числе к коммерческой тайне;

в 100% организаций доказана возможность получить привилегии администратора домена. Другими словами, злоумышленник будет способен выполнять любые действия в инфраструктуре компании, в том числе организовать подключение ко всем серверам и компьютерам;

в 85% уязвимости критического и высокого уровня опасности выявлены из-за слабых паролей;

в 60% компаний найдены уязвимости критического и высокого уровня опасности — они связаны с использованием устаревших версий софта;

35% уязвимостей оказались связаны с конфигурацией, 15% — с кодом веб-приложений.

В среднем на то, чтобы получить доступ во внутреннюю сеть организаций, пентестерам требовалось пять дней и четыре часа, а самая быстрая атака прошла за час». ***(Анастасия Марьина. IT-системы 96% крупных российских компаний оказались уязвимы для хакеров // РБточкаРУ (https://rb.ru/news/it-hacher-business/). 16.11.2022).***

***

«Країна-терорист росія досягла цифрового суверенітету, оскільки закордонні компанії залишили її ринок, розповів глава російської Мінцифри Максут Шадаєв на форумі «Цифровий алмаз».

«Якщо говорити про цифровий суверенітет, то ми його вже досягли, тому що іноземні компанії вже пішли з вітчизняного ринку. Ми тепер є самі в себе», — заявив міністр.

Він підкреслив, що від'їзд низки IT-фахівців з рф не завдав серйозної шкоди галузі. За його словами, механізми, що є в країні, мотивують багатьох залишатися і працювати тут. Нагадаємо, що на жовтень 2022-го року до Казахстану переїхали близько 50 000 російських айтішників, ще майже 12 000 втекли до Грузії.

Глава російської Мінцифри також зазначив, що російська IT-галузь має всі необхідні можливості для активного розвитку.

«Галузь, незважаючи на всі події останніх місяців, має всі необхідні можливості, щоб активно розвиватися та замінювати ті ніші, які звільняються у зв’язку з відходом іноземних компаній», — додав він». ***(В росії заявили про «досягнення цифрового суверенітету». Це значить, що майже всі IT-компанії покинули тамтешній ринок // Internetua (https://internetua.com/v-rosiyi-zayavili-pro-dosyagnennya-cifrovogo-suverenitetu-ce-znacsit-sxo-maije-vsi-it-kompaniyi-pokinuli-tamteshnii-rinok). 26.11.2022).***

***

Інші країни

«В то время как уверенность руководства в киберустойчивости падает во всем мире из-за значительного роста активности в последние годы, исследование Marsh и Microsoft, опубликованное в июне, показывает, что она

остается высокой в Азиатско-Тихоокеанском регионе, несмотря на то, что 64% предприятий сообщают, что они пострадали от кибератаки.

Рост числа атак, вызванных пандемией Covid-19, и быстрое внедрение цифровых услуг не поколебали уверенности 70% организаций в регионе, хотя почти половина признает, что еще есть возможности для улучшения. В опросе Microsoft/Marsh исследуется, является ли эта уверенность в киберустойчивости результатом действительно сильной оборонительной позиции или непониманием ландшафта угроз.

Исследование киберустойчивости: уверенность может быть утрачена, поскольку организации упускают из виду необходимые средства контроля

В опросе приняли участие 660 лиц, принимающих решения, по всему региону, занимающих должности от генерального директора до директора по информационной безопасности и управления рисками. Более 69 % заявили, что они уверены в программе управления рисками своей организации, несмотря на то, что более половины из них в настоящее время стали мишенью кибератак (и региональный уровень атак на 5 % выше, чем в среднем по миру). Однако этот оптимизм несколько умерен, так как только 11% заявили, что они «очень» уверены в своей киберустойчивости; еще 58% заявили, что они «достаточно» уверены.

48% респондентов сказали, что их программы нуждаются в некотором улучшении; если это совпадает с 31%, которые сказали, что они «не уверены» в своей киберустойчивости, это будет означать, что только 17% уверенных респондентов считают, что их программы в настоящее время имеют недостатки. Тем не менее, в опросе есть признаки того, что у гораздо большего числа могут быть проблемы, о которых они не знают.

Одна из них заключается в том, что региональная оценка киберриска значительно ниже среднемирового показателя. 63% респондентов по всему миру говорят, что они активно оценивают свой риск, но только 50% респондентов в Азии сообщают об этом. Кроме того, эти оценки имеют тенденцию быть скорее реактивными, чем проактивными; количество организаций в Азии, которые говорят, что проводят оценку после того, как кибератака или инцидент уже произошли, примерно вдвое превышает среднемировой показатель.

Азия также отстает в активном улучшении безопасности устройств, систем и сетей. 74% внесли улучшения в этой области в предыдущем году, что на первый взгляд может показаться разумным числом. Тем не менее, он отстает от среднемирового показателя в 91%. Это также несмотря на сообщения о том, что утечка данных и проблемы с конфиденциальностью были главной проблемой безопасности. Регион отстает в нескольких других категориях управления рисками: улучшении возможностей защиты данных, проведении тестов на проникновение и интеграции кибербезопасности в планы обеспечения непрерывности бизнеса. Тем не менее, он также опережает средний мировой показатель в ряде областей: переопределение ролей и обязанностей в области кибербезопасности в организациях, проведение оценок рисков поставщиков и цепочек поставок, проведение оценок перерывов в работе, внедрение DevSecOps и проведение анализов после кибератак.

По всем направлениям организации в Азии также отстают в реализации жизненно важных средств контроля рисков кибербезопасности: обнаружение конечных точек и реагирование на них, обучение по вопросам кибербезопасности и фишинга, хранение безопасных и зашифрованных резервных копий, фильтрация электронной почты и использование мер веб-безопасности.

Причины и решения

Почему организации в Азии, как правило, не проводят активную оценку своей киберустойчивости? Внутренний бизнес-консенсус примерно соответствует общемировому среднему, так что проблема не в этом. Большие различия заключаются в отсутствии данных и отсутствии таланта. У компаний в первую очередь возникают проблемы с наймом квалифицированных специалистов, необходимых для проведения оценок. Сюда входит оценка финансового риска, уровень которого составляет менее половины среднемирового показателя. Рынок экспертов по кибербезопасности практически везде ограничен для предприятий, но недавнее исследование ISC2 показало, что в Азии приходится почти две трети незаполненных вакансий в этом дефиците.

И когда это происходит, оценки киберустойчивости могут не соответствовать тому, что на самом деле присутствует в ландшафте угроз. Например, организации в Азии называют нарушения конфиденциальности своей самой большой проблемой, но результаты по всему миру показывают, что программы-вымогатели представляют собой самую большую угрозу.

Что можно сделать, чтобы закрыть эти пробелы в киберустойчивости? Исследование завершается рекомендацией сосредоточиться на расширенной аналитике и сравнительном анализе, количественной оценке финансового риска и регулярных оценках кибербезопасности. В нем также рекомендуются ключевые элементы управления, которые следует внедрить: многофакторная аутентификация, управление привилегированным доступом (PAM), фильтрация электронной почты, тестирование на фишинг и замена устаревших систем среди них.

Но руководитель практики Marsh Cyber Risk Practice Том Рейган предупреждает, что для повышения устойчивости требуется целостный подход; простая настройка одного-двух элементов или добавление пары новых функций безопасности существенно не исправит существующие недостатки. Рейган советует начать с улучшения взаимодействия между предприятиями, чтобы устранить пробелы и убедиться, что все отделы и сотрудники понимают свои конкретные обязанности по реагированию и защите». ***(Scott Ikeda. Confidence in Cyber Resilience Remains High in Asia-Pacific Despite Recent Increase in Attacks // CPO Magazine (https://www.cpomagazine.com/cyber-security/confidence-in-cyber-resilience-remains-high-in-asia-pacific-despite-recent-increase-in-attacks/). 11.11.2022).***

***

«Компания по развитию информационных и коммуникационных технологий (ИКТ) и инфраструктуры PPC Nigeria сообщила о недавних достижениях в области киберугроз в результате растущего внедрения новых технологий организациями и нескольких предупреждений и предупреждений

от Нигерийской комиссии по связи (NCC), в стране необходимо модернизировать критически важную инфраструктуру безопасности.

Глава отдела ИКТ компании PPC в Нигерии доктор Патрик Эде во время выступления в Лагосе заявил, что теперь киберпреступники используют сложные инструменты, чтобы получить контроль над устаревшими ИТ-системами и получить удаленный доступ к важным данным клиентов.

Следствием этого, по его словам, является то, что организации, безопасность которых была нарушена, столкнутся с нарушением критически важных операций, потерей доходов и важных данных.

Он заявил, что ущерб доверию и репутации, причиняемый действиями злонамеренных кибер-хакеров, часто бывает необратимым, добавив, что игнорирование уязвимостей в ИТ-системах может снизить общую эффективность бизнеса.

Группа реагирования на инциденты компьютерной безопасности NCC (CSIRT) за последние месяцы выпустила различные предупреждения безопасности, призывая нигерийцев остерегаться пяти вредоносных расширений Google Chrome, скомпрометированных приложений и уязвимостей в определенных антивирусных продуктах, которые тайно отслеживают действия пользователей в Интернете и ставят под угрозу их данные.

Регулятор телекоммуникационных услуг заявил, что вредоносные программы, которые могут нанести большой ущерб, были загружены несколько раз ничего не подозревающими людьми и, следовательно, поставили под угрозу конфиденциальность пользователей.

«Компании сталкиваются с новыми угрозами безопасности, возникающими из-за беспрецедентного глобального внедрения технологий и гибридной культуры работы. Эти преступники исследуют уязвимости в новых и существующих технологических установках, чтобы начать свои атаки», — сказал Эде.

Он добавил: «Организациям стало необходимо переосмыслить то, как они решают проблемы безопасности. Регулярное обновление программной и аппаратной инфраструктуры должно быть включено в меры кибербезопасности, чтобы свести к минимуму риск взломов. Программное обеспечение не идеально, и злоумышленники часто используют лазейки.

Следовательно, предприятия должны планировать развертывание исправлений сразу после того, как поставщик объявит об угрозе безопасности.

«Несмотря на то, что большое внимание уделяется обновлениям программного обеспечения, физические технологические устройства, такие как рабочие станции и серверы, которые работают медленно или перестали получать обновления от поставщиков, необходимо заменить, чтобы снизить риск утечки данных. Большая часть аппаратной инфраструктуры с истекшим сроком службы несовместима с новыми установками программного обеспечения, и поэтому для работы программного обеспечения требуется обновленное оборудование».

Он сказал, что опыт PPC Nigeria в развертывании ИКТ и инженерных решений помог нескольким организациям в государственном и частном секторах создать безопасную и совместную рабочую среду». ***(Adeyemi Adepetun. PCC advocates upgrade of critical security infrastructure against rising cyber-threats // GUARDIAN***

Newspapers (https://guardian.ng/business-services/pcc-advocates-upgrade-of-critical-security-infrastructure-against-rising-cyber-threats/). 10.11.2022).

***

«2022 год — знаменательный год для развития законов о конфиденциальности данных и кибербезопасности в Юго-Восточной Азии…

Индонезия

Новые законы о конфиденциальности данных в Индонезии

Долгожданный Закон о защите персональных данных (« PDPL») действует с октября 2022 года. PDPL — это первый всеобъемлющий закон о защите данных в Индонезии. У организаций будет 2-летний переходный период для соблюдения PDPL.

Все существующие законы и нормативные акты, регулирующие защиту персональных данных, останутся в силе в той мере, в какой они не противоречат положениям ЗПОД (включая требования к локализации данных в соответствии с Постановлением Правительства № 71 от 2019 г., поскольку локализация данных не регулируется ЗПОД). Мы ожидаем, что в ближайшие месяцы будут приняты постановления, содержащие рекомендации по ключевым аспектам PDPL.

Между PDPL и Общим регламентом ЕС по защите данных (« GDPR ») есть сходства и различия:

PDPL принимает понятия «субъект данных», «контролер данных» и «обработчик данных» и требует обязательного уведомления властей о нарушениях в течение 3 дней (значительно меньше, чем 14-дневный период в соответствии с предыдущим режимом).

Правовые основания для обработки персональных данных аналогичны тем, которые предусмотрены GDPR. Помимо согласия субъектов данных, альтернативные правовые основания включают необходимость заключения договора, юридические обязательства, защиту жизненно важных интересов субъекта данных и законных интересов контролера (среди прочего). Наличие альтернативных правовых оснований является существенным отходом от прежнего режима, который требовал согласия почти во всех случаях.

Экстерриториальная сфера действия PDPL шире, чем в GDPR, в том смысле, что она не ограничивается определенными условиями срабатывания. Контроллеры и обработчики персональных данных, расположенные за пределами Индонезии, должны соблюдать PDPL, если они обрабатывают персональные данные в Индонезии, и такая обработка имеет «юридические последствия» для Индонезии или кого-либо в Индонезии. Нет никаких указаний относительно того, что означает «правовое воздействие» в соответствии с PDPL.

Исключения из применения PDPL аналогичны исключениям в других юрисдикциях, например, когда персональные данные обрабатываются в личных или домашних целях, а обработка данных осуществляется в (a) интересах национальной обороны и безопасности; (б) интересы правоприменительного процесса; (c) общественный интерес в контексте государственного управления; или (d) интересы надзора за финансовыми услугами, денежно-кредитным сектором, платежной

системой и стабильностью финансовой системы, осуществляемые в контексте государственного управления.

Механизмы передачи для трансграничной передачи данных аналогичны механизмам в других юрисдикциях, но перечислены в порядке приоритета следующим образом: (i) решение об адекватности (т.е. сопоставимый уровень защиты); (ii) обязательные договорные положения для зарубежного получателя данных; и (iii) согласие субъектов данных. Это значительное послабление по сравнению с предыдущей системой, которая требует предварительного и последующего уведомления Министерства связи и информатики. Еще неизвестно, выпустит ли регулирующий орган типовые договорные положения для (ii) в соответствии с будущими правилами.

Новый режим санкций устанавливает ряд уголовных и административных штрафов разной величины в зависимости от характера нарушения. Уголовные санкции включают штрафы в размере до 400 000 долларов США для физических лиц и 4 миллиона долларов США для корпораций, а также лишение свободы на срок до 6 лет для физических лиц. Уголовные санкции могут быть наложены на совет директоров и бенефициарных владельцев компаний. На виновную сторону может быть наложен административный штраф в размере до 2% ее годового оборота. Этими санкциями правительство посылает убедительный сигнал о том, что в Индонезии необходимо серьезно относиться к защите персональных данных.

Пожалуйста, обратитесь к нашему полному брифингу.

Таиланд

Законы о конфиденциальности в Таиланде собираются вместе

В Таиланде было введено несколько руководств с разными датами вступления в силу, поскольку основные положения о защите данных в соответствии с Законом о защите персональных данных (« PDPA ») вступили в силу 1 июня 2021 года. Организации в Таиланде должны рассмотреть новые правила, чтобы гарантировать, что их данные практика конфиденциальности остается в соответствии с PDPA.

Руководство по запросу согласия от субъекта данных в соответствии с Законом о защите персональных данных E. 2562 (2019) (« Руководство по получению согласия»), опубликованное 7 сентября 2022 года, устанавливает подробные требования для получения действительного согласия от физических лиц, включая сроки и информацию, которую необходимо предоставить. к субъектам данных.

Руководство по процедурам уведомления о целях и деталях, касающихся сбора персональных данных от субъектов данных в соответствии с Законом о защите персональных данных. 2562 (2019) («Руководство по уведомлению») устанавливает принципы для организаций при предоставлении уведомления субъекту данных о том, как обрабатываются его персональные данные.

Уведомление об освобождении МСП от обязанностей по ведению документации («Руководство ROPA») устанавливает минимальную информацию, которая должна быть включена в записи ROPA.

Комитет по защите персональных данных («PDPC») в настоящее время проводит публичные слушания по проекту уведомления о трансграничной передаче персональных данных («Проект уведомления»), которое дополнит PDPA в отношении трансграничной передачи персональных данных. за пределами Таиланда.

Проект уведомления следует подходу GDPR и устанавливает требования в отношении обязательных корпоративных правил и других мер безопасности, включая стандартные договорные положения, кодексы поведения и сертификацию. Слушание продлилось до 24 октября 2022 года.

Несмотря на то, что в соответствии с PDPA существует положение о дедушке, которое позволяет контролерам данных продолжать обработку персональных данных, которые были собраны до 1 июня 2021 года, контролеры данных обязаны публиковать каналы, с помощью которых субъекты данных могут помешать контролерам данных делать это.

Вьетнам

Указ 53, наконец, вносит некоторую ясность в Закон о кибербезопасности.

Указ № 53/2022/ND-CP (« Указ 53»), вступивший в силу 1 октября 2022 г., разъясняет некоторые важные аспекты Закона о кибербезопасности № 24/2018/QH14 («Закон о кибербезопасности»), в том числе применение требований по локализации данных к юридическим лицам, зарегистрированным во Вьетнаме, и иностранным предприятиям.

Критерии в соответствии с Законом о кибербезопасности и Указом 53 вместе предусматривают, что требования к локализации данных применяются только к организациям, зарегистрированным во Вьетнаме, которые являются: (i) поставщиками услуг в телекоммуникационной сети, Интернете или предоставляющими услуги с добавленной стоимостью в киберпространстве; и (ii) обработка персональных данных пользователей во Вьетнаме, данных об отношениях пользователей во Вьетнаме или данных, созданных пользователями во Вьетнаме. Отечественное юридическое лицо должно хранить такие указанные категории данных во Вьетнаме на неопределенный срок. Мы знаем из Министерства общественной безопасности, что можно отразить такие данные на локальном сервере и хранить копию личных данных за пределами Вьетнама.

Для иностранных предприятий Указ 53 разъясняет, что такие указанные категории данных должны храниться во Вьетнаме, а местное присутствие необходимо устанавливать только при соблюдении всех следующих условий:

- компания работает в предписанном секторе, связанном с киберпространством, что означает, среди прочего, телекоммуникационные услуги, услуги по хранению и обмену данными в киберпространстве, услуги электронной коммерции и онлайн-платежей (« Определенные услуги»);
- имеет место нарушение Закона о кибербезопасности при оказании Указанных услуг;
- несоблюдение уведомления или запроса Департамента кибербезопасности и предотвращения преступлений в сфере высоких технологий («DCPHC»); а также
- DCPHC выдает запрос на локализацию данных и установление локального присутствия.

Закон о кибербезопасности требует, чтобы отечественные и иностранные поставщики услуг хранили данные пользователей во Вьетнаме. Это требование

вызвало обеспокоенность у организаций из-за его двусмысленности, в том числе в отношении объема требований к локализации данных.

Хотя Указ 53 полезен для разъяснения некоторых аспектов Закона о кибербезопасности, в соответствии с Указом 53 всегда должно быть получено согласие субъекта данных, поскольку нет другой альтернативной правовой основы для обработки его данных. Кроме того, Указ 53 не содержит каких-либо пороговых значений для уведомляемых утечек данных, что означает, что все типы утечек данных подлежат уведомлению PDPC.

Индия

Ожидаем ли мы полного пересмотра индийских законов о защите данных?

3 августа 2022 года Индия отозвала законопроект о защите персональных данных, внесенный в 2019 году. Отмененный законопроект был подробно рассмотрен парламентом Индии с более чем 80 поправками и 12 рекомендациями, предложенными до отзыва. Ожидается, что новый законопроект о защите данных будет представлен на утверждение парламенту Индии в декабре 2022 года.

Ключевые области, вызывающие озабоченность в рамках отмененного законопроекта, включают управление конфиденциальной информацией и объем доступа правительства Индии к данным.

Сингапур

(i) Эмоциональный дистресс, признанный убытком или ущербом, подлежащим судебному преследованию

Апелляционный суд Сингапура постановил, что эмоциональный стресс может представлять собой «утрату или ущерб» в соответствии с Законом о защите персональных данных 2012 года («PDPA»). При определении того, является ли эмоциональное расстройство формой потери или ущерба, Апелляционный суд по делу Рид, Майкл против Беллингема, Алекс (генеральный прокурор, вмешавшийся) [2022] SGCA 60 обнаружил, что более широкое толкование PDPA лучше способствует достижению целей PDPA и этот парламент намеревались сделать принудительный режим PDPA эффективным средством, с помощью которого люди могут обеспечить соблюдение своих прав на защиту своих личных данных. Суд постановил, что потеря контроля над личными данными не является потерей или ущербом для целей PDPA.

(ii) Новый административный штраф в размере до 10% годового оборота организации в Сингапуре.

Административный штраф за утечку данных в соответствии с PDPA, который составляет до 10% годового оборота организации в Сингапуре (если годовой оборот превышает 10 миллионов сингапурских долларов), вступил в силу 1 октября 2022 года в соответствии с поправками, изложенными в Законе о защите персональных данных (поправка) Закон 2020 г. Организации будут потенциально нести ответственность за штрафы за нарушение требований к защите персональных данных в соответствии с PDPA (за исключением части 9 и раздела 48B(1) PDPA).

Малайзия

Реформа закона о конфиденциальности вынесена на обсуждение парламента Малайзии

В Малайзии в настоящее время нет требования об обязательном уведомлении об утечке данных в соответствии с законодательством о конфиденциальности данных, Законом о защите персональных данных 2010 г. («PDPA»). Реформы по внедрению режима обязательного уведомления об утечке данных были вынесены на обсуждение парламента в октябре 2022 года.

Предлагаемый режим обязательного уведомления данных был одной из 22 рекомендаций в документе для консультаций с общественностью PDPA, опубликованном Комиссией по защите персональных данных («PDPC») в феврале 2020 года.

Предлагаемый режим обязательного уведомления об утечке данных потребует, чтобы о подлежащих уведомлению утечках персональных данных сообщалось в PDPC в течение 72 часов. PDPC предлагает выпустить руководство, чтобы помочь организациям соблюдать это новое требование об обязательном уведомлении.

Сообщается, что другие рекомендации, представленные для обсуждения в парламенте, включают: (i) наложение прямого обязательства на обработчиков данных соблюдать принципы безопасности в соответствии с PDPA; (ii) назначение сотрудника по защите данных; (iii) закрепление прав на переносимость данных, т.е. пользователь данных должен передавать персональные данные субъекта данных другому пользователю данных в удобном для пользователя машиночитаемом формате по запросу субъекта данных (если это технически возможно); и (iv) «черный список» юрисдикций для трансграничных переводов Малайзии (для замены существующей предписывающей системы «белых списков»).

Филиппины

Новые подходы к определению штрафов в соответствии с законами о конфиденциальности данных

Недавнее введение Циркуляра NPC № 2022-01 (« Циркуляр») о Руководстве по административным штрафам показывает, что Филиппины применяют новый подход к определению штрафов за нарушение Закона о конфиденциальности данных 2012 года.

Руководство устанавливает три категории нарушений, а именно: (i) серьезные нарушения; (ii) серьезные нарушения; и (iii) другие нарушения. Нарушения классифицируются по:

количество затронутых субъектов данных;

частота нарушений; а также

причина несоблюдения (например, недосмотр, безрассудство или преднамеренные действия).

«Тяжелые правонарушения» и «крупные правонарушения» влекут за собой административный штраф в размере определенного процента годового валового дохода правонарушителя (т.е. от 0,5% до 3% и от 0,25% до 2% соответственно). «Другие нарушения» влекут за собой наложение штрафа в размере от 50 000 песо (870 долларов США) до 200 000 песо (3 500 долларов США)…» ***(Key changes in data privacy and cyber security laws across Southeast Asia in 2022 // Herbert Smith Freehills (https://hsfnotes.com/data/2022/11/15/key-changes-in-data-privacy-and-cyber-security-laws-across-southeast-asia-in-2022/). 15.11.2022).***

***

«Приблизительно 6,74 миллиона случаев кибербезопасности были зарегистрированы до июня 2022 года в Индии, как сообщил государственный министр по электронике и информационным технологиям Раджив Чандрасекар в парламенте 20 июля 2022 года.

Жизнь стала невероятно простой благодаря цифровому веку, когда информацию можно обрабатывать и передавать за наносекунды, а машины можно запускать и останавливать прикосновением пальца.

Цифровая эра потрясла нашу стремительную жизнь. Но и здесь есть подвох!

Мы должны понимать, что технологии развиваются для всех нас — как для законопослушных пользователей компьютеров, так и для хакеров или киберпреступников. Воспринимайте это как дом, двери и окна которого легко проходимы, и поэтому грабители также могут проникнуть внутрь без надлежащей проверки безопасности.

Вот некоторые из наиболее распространенных форм кибератак, наблюдавшихся в период 2018–2022 годов:

Вредоносное ПО или программы-вымогатели. Нежелательное программное обеспечение, которое было установлено на ваш компьютер против вашей воли, называется вредоносным ПО. Он может дублировать себя по всему Интернету, прятаться в полезных приложениях, помечать легальный код и распространяться. Примеры включают макровирусы, файловые инфекторы, трояны, черви, дропперы, логические бомбы, программы-вымогатели и т. д. Семьдесят восемь процентов индийских фирм, зашифровавших данные, должны были заплатить выкуп, чтобы вернуть их, даже если у них были резервные копии или другие способы получения данных. восстановление (Sophos, 2022).

Фишинг. Отправка электронных писем из, казалось бы, надежных источников для получения личной информации получателей называется фишингом. Он сочетает в себе обман на технологическом и социальном уровнях. Это может повлечь за собой загрузку вредоносного ПО на ваш компьютер через вложение электронной почты или переход по ссылке на поддельный веб-сайт. Примеры включают китобойный промысел, смишинг, вишинг, мошенничество с генеральным директором, фарминг, внедрение контента, мошенничество с сообщениями от крупной рекламной кампании и т. д. Во втором квартале 2022 года в Индии ежедневно совершалось более 17,5 тысяч фишинговых атак через социальные сети (Siasat)., 2022).

Человек посередине: когда хакер берет на себя управление сеансом между клиентом и сетевым сервером, происходит атака MitM. Компьютер хакера подделывает порядковые номера клиентов и заменяет их IP-адреса собственным. Сервер думает, что он все еще находится на связи с клиентом, поскольку компьютер хакера продолжает общаться с сервером. Наиболее типичная атака MitM включает в себя предоставление широкой публике бесплатных вредоносных точек доступа Wi-Fi.

Выкачивание 94,42 крор индийских рупий из Cosmos Bank в Пуне в 2018 году, вторжение DTrack RAT в системы завода в Куданкуламе в 2019 году, блокировка Google 240 миллионов спамеров и 18 миллионов онлайн-мошенников в 2020 году,

CAT приводит дело о краже со взломом в 2021 году и требование выкупа в размере 75000000 долларов США. совершенные Oil India Ltd в 2022 году, — это лишь некоторые из громких киберпреступлений, которые произошли за последние 4 года и вызывают большое беспокойство у Индии.

Нехватка навыков приводит к кибернезащищенности?

Дело в том, что киберпреступники быстро становятся более изощренными, чем обычные пользователи, в применении новейших технологий, таких как Интернет вещей, искусственный интеллект, машинное и глубокое обучение, облачное шифрование, встроенная аппаратная аутентификация, сети 5G, поведенческая аналитика, квантовые вычисления и т. д. и в этом заключается большая часть проблемы.

Согласно отчету ISACA о состоянии кибербезопасности за 2022 год, 40% предприятий утверждают, что их команда по кибербезопасности недоукомплектована, в то время как 60% предприятий в Индии имеют открытые роли в области кибербезопасности.

Что ты можешь сделать?

Довольно интересно отметить, что такая страна, как Индия, которая экспортирует ИТ-специалистов, также сталкивается с дефицитом навыков кибербезопасности дома и за рубежом. Корпоративные проблемы существуют также, если есть проблема с исполнением правительства.

Технология не проблема; образование есть. Изучение кибербезопасности является развивающейся областью. Это требует образования и перевоспитания. Поэтому учебная программа должна регулярно обновляться, чего в настоящее время не происходит. В результате студенты, вступающие в реальный мир работы, не справляются с поставленными задачами.

Ниже приведены некоторые советы, которые обычный пользователь может легко использовать, чтобы стать безопаснее в Интернете:

- Выход из системы, когда он не используется: заблокируйте или отключите свой смартфон, ноутбук или любое другое подключенное устройство, когда оно не используется, чтобы предотвратить несанкционированный доступ.
- Менеджер паролей: используйте один из надежных генераторов паролей, чтобы защитить свои устройства с помощью специального пароля.
- Избегайте использования общественного Wi-Fi: бесплатный Wi-Fi может быть доступен в столовых, ресторанах и других общественных местах, но имейте в виду, что он бесплатный для всех, включая кибер-злоумышленников.

Доступные учебные программы по кибербезопасности не очень хорошо рекламируются в Индии, даже из надежных источников. Лучшие студенты до сих пор не осознают прибыльности сферы кибербезопасности. Результат? Они все чаще переезжают за границу для обучения кибербезопасности в поисках более высокой отдачи от инвестиций.

Индия должна внедрить изменения с нуля, если она хочет удовлетворить спрос на профессионалов в области кибербезопасности и улучшить нынешнюю киберситуацию». ***(Abhishek Agarwal. Rising cyber security risk due to skill shortage // Bennett, Coleman & Co. Ltd. (https://timesofindia.indiatimes.com/blogs/voices/rising-cyber-security-risk-due-to-skill-shortage/). 26.11.2022).***

***

«ЕС объявляет Россию террористическим государством; Атака последовала за DDoS-атаками на восточные страны

Прокремлевские хакеры KillNet взломали веб-сайт Европарламента в среду в результате DDoS-атаки, которая произошла всего через несколько часов после того, как законодательный орган объявил Россию террористическим государством. Веб-сайт все еще был недоступен в конце дня из-за череды атак хактивистов на восточноевропейские и балканские государства.

Жауме Дюч, представитель Европейского парламента, написал в Твиттере в среду, что веб-сайт пострадал «из-за высокого уровня внешнего сетевого трафика», который он обвинил в распределенной атаке типа «отказ в обслуживании».

Официальный сайт Европарламента по состоянию на полдень среды не работал. Дач говорит, что агентство в настоящее время работает над тем, чтобы быстро решить проблему.

В среду ответственность за взлом взяла на себя прокремлевская хакерская группа KillNet.

«Страпоновый обстрел серверной части официального сайта Европарламента!» группа разместила в своем Telegram-канале.

Атаки на Европейский парламент произошли через несколько часов после того, как агентство приняло резолюцию, официально признающую Россию государством-спонсором терроризма. Он был принят государствами-членами 494 голосами против 58 при 44 воздержавшихся.

Европейский парламент также призвал ЕС ввести дополнительные санкции против России, чтобы изолировать страну на международном уровне за ее военные преступления против Украины.

KillNet входит в число немногих российских киберпреступных группировок, открыто присягнувших Москве. Группа, название которой происходит от инструмента, который можно было использовать для запуска DDoS-атак, превратилась в прокремлевских хактивистов.

С самого начала российского вторжения в Украину KillNet активно вербует добровольцев, часто объединяя их в разные отряды с такими именами, как «Кратос», «Райд» и «Заря», для проведения DDoS-атак против западных стран (см. - Московские хакеры заявляют о DDoS-атаке на сайт ФБР).

Группа провела аналогичные DDoS-атаки на веб-сайт Сената Польши в октябре после того, как польская палата единогласно проголосовала за признание России «террористическим режимом». Парламентские ИТ-системы).

По данным Института CyberPeace, который отслеживает публично раскрытые атаки, связанные с войной между Россией и Украиной, KillNet провела 76 атак на проукраинские страны с начала войны в феврале.

Получить комментарий в Европарламенте не удалось». ***(Akshaya Asokan. Russian KillNet Shuts Down EU Parliament Website With DDoS // Information Security***

Media Group, Corp. (https://www.govinfosecurity.com/russian-killnet-shuts-down-eu-parliament-website-ddos-a-20541). 23.11.2022).

***

«Премьер-министр Австралии заявил, что Россия должна «нести ответственность» за утечку данных

Австралийская полиция заявляет, что группа свободно связанных киберпреступников, базирующихся в России, вероятно, несет ответственность за взлом Medibank, крупнейшей частной страховой компании страны.

Комиссар федеральной полиции Австралии Рис Кершоу заявил сегодня днем журналистам, что власти считают, что они установили личности преступников и намерены провести переговоры о них с российскими правоохранительными органами.

«Эта кибератака является неприемлемой атакой на Австралию, и она заслуживает ответа, соответствующего злонамеренным и далеко идущим последствиям, которые вызывает это преступление», — сказал Кершоу. AFP предпринимает скрытые меры и круглосуточно работает с нашими внутренними агентствами и нашими международными сетями, включая Интерпол».

Хакеры могут быть повторным запуском банды вымогателей REvil или чем-то еще, известным как BlogXX.

Хакеры начали утечку данных, в том числе электронную таблицу под названием «Boozy.csv» и другую под названием «abortions.csv». Ранее они публиковали образцы данных, отсортированные по «непослушным» и «хорошим» спискам. Последние содержали имена, связанные с диагностическими кодами медицинских проблем, таких как опиоидная зависимость.

Комментарии Кершоу прозвучали после того, как премьер-министр Австралии Энтони Альбанезе заявил журналистам, что «страна, из которой исходят эти атаки, также должна нести ответственность за отвратительные атаки и публикацию информации, включая очень личную и конфиденциальную информацию».

«Мы знаем, откуда они поступают, мы знаем, кто несет ответственность, и мы говорим, что они должны быть привлечены к ответственности», — сказал Альбанезе. Ранее он сообщил журналистам, что его личная информация как клиента Medibank может быть включена в Нет никаких признаков того, что его данные просочились в сеть.

Medibank заявил в понедельник, что не будет платить хакерам по требованию выкупа, сообщив 9,7 миллионам человек, чьи данные были обнаружены в результате инцидента, что шансы вымогателей на самом деле вернуть свои данные «ограничены».

Общее число пострадавших составляет 5,1 миллиона клиентов Medibank, около 2,8 миллиона клиентов ahm и около 1,8 миллиона международных клиентов, которым требуется частное медицинское страхование во время проживания или учебы в Австралии.

В этих итогах содержатся данные о заявлениях о здоровье для 160 000 клиентов Medibank, около 300 000 клиентов и около 20 000 международных клиентов. Эти данные включают коды, связанные с диагнозами и процедурами.

Хакеры заявили, что их первоначальный запрос составлял 10 миллионов долларов, но они готовы снизить его до 9,7 миллиона долларов, или по 1 доллару за каждую запись. Генеральный директор Medibank Дэвид Кочкар сказал, что фактическая цифра в долларах «не имеет значения».

Австралийская полиция заявляет, что примет «незамедлительные меры» против любого, кто воспользуется просочившимися данными Medibank». ***(Mihir Bagwe. Australia Blames Russian Hackers for Medibank Hack // Information Security Media Group, Corp. (https://www.govinfosecurity.com/australia-blames-russian-hackers-for-medibank-hack-a-20452). 11.11.2022).***

***

«Геополитика вызывает серьезные изменения в ландшафте угроз

Поддерживаемые государством хакерские группы будут уделять больше внимания операционным технологиям, поскольку геополитика влияет на ландшафт киберугроз, говорится в отчете Агентства кибербезопасности Европейского Союза, опубликованном в четверг.

«Сегодняшний глобальный контекст неизбежно приводит к серьезным изменениям в ландшафте угроз кибербезопасности. Новая парадигма формируется за счет растущего числа участников угроз. Мы вступаем в фазу, которая потребует соответствующих стратегий смягчения последствий для защиты всех наших критических секторов, наших все граждане ЕС», — заявил исполнительный директор ENISA Юхан Лепассаар. В отчете анализируются киберинциденты во второй половине 2021 года и первой половине 2022 года и делаются некоторые прогнозы на ближайшее будущее.

Доказательства, приводимые агентством о растущем интересе государства к взлому ОТ, включают обнаружение в апреле вредоносного ПО, получившего название Industroyer2, фирмой по кибербезопасности Eset, которое использовалось при попытке заражения высоковольтных электрических подстанций в Украине. В этом месяце также был обнародован инструмент для атак, получивший название Incontroller. Анализ, проведенный Mandiant и Schneider Electric, показал, что Incontroller «весьма вероятно, спонсируется государством и содержит возможности, связанные с нарушением работы, саботажем и, возможно, физическим уничтожением» устройств автоматизации машин.

По подсчетам ENISA, Industroyer2 и Incontroller являются пятым и шестым известными примерами вредоносного ПО для промышленных систем управления.

«По нашим оценкам, поддерживаемые государством субъекты угроз активизируют свою разведку в отношении сетей ОТ, развивают возможности и все чаще нацеливаются на них в обозримом будущем, особенно во время кризисов и вооруженных конфликтов», — говорится в отчете агентства по кибербезопасности.

Агентство также отмечает, что поддерживаемые государством субъекты угроз все больше внимания уделяют компрометации цепочки поставок. Фирмы частного сектора, занимающиеся кибербезопасностью, сообщают о значительном увеличении за последние три года правительственных взломов таких целей, как поставщики управляемых услуг и организации ИТ-услуг, с целью закрепиться в сетях сотен жертв.

Хотя кибервойна, спровоцированная вторжением России в Украину, которой так опасаются, еще не материализовалась, ENISA заявляет, что по-прежнему вероятно, что западные страны и союзники по НАТО расценят кибератаки на критически важную инфраструктуру как возмездие за поддержку Киева.

Одна из возможностей состоит в том, что пророссийские банды вымогателей проводят ответные меры по указанию Кремля, в том числе используя вредоносные программы-вымогатели, чтобы замаскировать присутствие Кремля и дать Москве правдоподобное отрицание.

Само ПО-вымогатели — исключительно по финансовым мотивам — конечно, продолжает оставаться проблемой.

Группы, стоящие за штаммами программ-вымогателей, реагируют на усиление правоохранительных органов тем, что якобы уходят из криминального подполья только для того, чтобы вернуться с новым прозвищем. ENISA прогнозирует, что эта тенденция сохранится, но группы программ-вымогателей как услуги будут приобретать более мелкие группы уровней, что может привести к частичному использованию различных вариантов программ-вымогателей». ***(Akshaya Asokan. More State-Sponsored OT Hacking To Come, Says ENISA // Information Security Media Group, Corp. (https://www.govinfosecurity.com/more-state-sponsored-ot-hacking-to-come-says-enisa-a-20398). 03.11.2022).***

***

«Когда кибератака — это кибервойна, которую судят спустя пять лет после NotPetya Wave

Четырехлетняя судебная тяжба по поводу того, была ли атака NotPetya, в целях страхования, актом войны, подошла к концу в зале суда Чикаго, в то время как другие юридические споры о том, когда кибер-инцидент является актом войны, остаются нерешенными.

Mondelez International — производитель печенья Oreo, крекеров Ritz и порошка с фруктовым вкусом Tang — подала в суд на Zurich Insurance Group в 2018 году после того, как андеррайтер отклонил иск производителя продуктов питания в соответствии с полисом страхования собственности на сумму не менее 100 миллионов долларов в качестве компенсации за ущерб, вызванный волной вредоносного ПО.

В кратком заявлении Zurich Insurance Group подтвердила, что судебный процесс в суде штата Иллинойс между двумя сторонами завершился в конце октября. «Стороны взаимно урегулировали вопрос», — сказал представитель.

Mondelez не ответил на запрос о комментариях. Law360 сообщил, что судья Мэри Робертс удовлетворила ходатайство, выдвинутое обеими сторонами, о окончательном прекращении судебного процесса, при этом каждая сторона несет свои собственные расходы. Ходатайство поступило незадолго до того, как заключительные аргументы должны были начаться в суде присяжных уже на второй неделе.

В своей жалобе от 2018 года Mondelez заявила, что Zurich отказал в покрытии страхового полиса за физическую потерю или ущерб, включая электронные данные,

сославшись на пункт, исключающий ущерб, причиненный «враждебными или военными действиями».

В сообществах кибербезопасности и страховых компаний внимательно отслеживали судебный процесс на предмет того, как он повлияет на корпоративные подходы к киберрискам. Страховая площадка Lloyd's of London ранее в этом году сообщила андеррайтерамначать исключать покрытие кибератак, связанных с войной или катастрофическими атаками, вызванными государством. Неясно, в какой степени разрушительные атаки, инициированные хакерскими группами национального государства, могут быть исключены из покрытия, не оказывая давления на рынок киберстрахования, учитывая, как NotPetya продемонстрировал, что атака, направленная на определенные цели, может быстро выйти из-под контроля, и в целом более низкий порог для выражения национальной агрессии в виртуальном и физическом пространстве. Правительство США в сентябре инициировало исследование того, должно ли оно обеспечить поддержку или другой механизм, гарантирующий, что кибератаки с катастрофическими последствиями не останутся незастрахованными.

«Я определенно думаю, что вы увидите, что держатели полисов гораздо больше устанут платить большие деньги за такое покрытие, если оно не будет включать в себя поддерживаемые государством кибератаки», — сказала Джозефин Вольф, академик Университета Тафтса, изучающая рынок киберстрахования. По ее словам, победа страховщиков, исключающая ответственность страховщиков за кибератаки на уровне государства, также спровоцирует новые судебные разбирательства по поводу атрибуции. Она отметила, что четкая принадлежность NotPetya к России — редкость среди киберинцидентов.

NotPetya был задуман российской военной разведкой как атака, нацеленная на украинский бизнес через приложение для налогового учета, широко используемое в этой восточноевропейской стране. Вместо этого он распространился по всему миру, а ущерб обычно оценивается примерно в 10 миллиардов долларов. Представитель Кремля в 2018 году оспорил российскую атрибуцию вредоносного ПО, заявив СМИ, что приписывание Москвы правительством Великобритании и другими союзниками США было частью «русофобской кампании».

Федеральная прокуратура в 2020 году предъявила обвинения шести российским военным в связи с NotPetya и другими хакерскими инцидентами.

Mondelez говорит, что вредоносное ПО достигло двух серверов, расположенных в разных физических местах и в разное время, и в конечном итоге навсегда вывело из строя 1700 серверов и 24 000 ноутбуков.

Адвокаты Цюриха заявили, что ИТ-инфраструктура Mondelez была «побочным ущербом» от многолетней агрессии России против Украины, сообщает Law360.

Mondelez — не единственная крупная американская компания, которая обнаружила, что требования о возмещении ущерба NotPetya отклонены страховщиком, ссылающимся на исключения за военные действия. Фармацевтический гигант Merck с 2018 года находится в судебном процессе в суде штата Нью-Джерси против своих страховщиков после того, как попытался потребовать возмещения убытков на сумму 1,4 миллиарда долларов от своих

поставщиков страхования имущества. Судья Томас Уолш в декабре вынес решение в пользу Merck, заявив, что компания «имела полное право предвидеть, что исключение распространяется только на традиционные формы ведения войны».

Адвокаты Mondelez, возможно, обратили внимание на это решение, сказал Вольф, назвав это решение возможным мотивом для мирового соглашения.

Дело Merck все еще открыто, и страховые ответчики быстро подали апелляцию». ***(David Perera. Oreo Maker Settles With Insurer Over NotPetya Damages Claim // Information Security Media Group, Corp. (https://www.govinfosecurity.com/oreo-maker-settles-insurer-over-notpetya-damages-claim-a-20396). 02.11.2022).***

***

«К 2027 году оборонные ведомства должны внедрить стандарты нулевого доверия.

У оборонных ведомств есть время до 2027 года, чтобы преобразовать свои сети в архитектуры, которые постоянно проверяют, чтобы убедиться, что никто не получает доступ к данным, которым они не должны.

Этот переход к принципам нулевого доверия лежит в основе нового пятилетнего плана Пентагона по защите своих информационных систем от кибератак. Стратегия и дорожная карта были опубликованы во вторник.

Чтобы достичь этого, агентства могут улучшить свои существующие среды, внедрить коммерческое облако, которое уже соответствует спецификациям Министерства обороны США с нулевым доверием, или скопировать прототип частного облака, сообщил журналистам Дэвид МакКаун, исполняющий обязанности главного заместителя директора по информационным технологиям Пентагона. И чтобы помочь обеспечить его соблюдение, главный информационный офис Министерства обороны США будет отслеживать их расходы.

«Мы привлечем их к ответственности, попросив разработать план», — сказал МакКевон. «И в рамках этого руководства по планированию возможностей… они должны вернуться к нам и показать нам в своих бюджетах, сколько они тратят на нулевой уровень доверия и что они получают за это».

МакКаун сказал, что реализация не должна сильно изменить пользовательский опыт, за исключением дополнительных шагов аутентификации, чтобы убедиться, что нужные люди получают доступ к информации.

«Возможно, мы используем теги данных, и для доступа к определенным фрагментам данных может потребоваться дополнительная аутентификация. Но мы бы предпочли, чтобы было очень мало трения, когда пользователь занимается своими повседневными делами», — сказал он.

Но частью достижения универсальной позиции нулевого доверия является управление идентификацией, учетными данными и доступом, или ICAM.

«Не все в отделе используют федеративное решение ICAM, с которым мы можем сверить учетные данные. Это будет отправной точкой», — сказал он, добавив, что, вероятно, будет проведено некоторое обучение концепциям нулевого доверия.

DOD планирует отслеживать внедрение и производительность продукта в своих 10 000 информационных системах, сказал МакКаун, отвечая на такие вопросы,

как «Все ли было обнаружено? Как быстро мы могли ответить? Как быстро мы можем восстановить окружающую среду?»

Кибертестирование будет продолжаться по мере создания системы и после использования автоматизированных инструментов. Кроме того, ожидается, что обновления сети будут выполняться во время реализации нулевого доверия.

Растущая зависимость Министерства обороны от коммерческой облачной инфраструктуры вызвала критику, связанную с кибербезопасностью. Но МакКаун сказал, что нулевое доверие было «заметной дискуссией в зале о возможностях поставщиков и о том, смогут ли они поставить», будь то повседневные компьютеры, оружие или промышленные системы управления.

В качестве первого шага в многолетнем путешествии Министерство обороны собирается начать пилотное внедрение принципов нулевого доверия с облачной архитектурой. Но успех не является данностью.

«Все начинают думать об этих концепциях нулевого доверия и внедрять их в решения, которые мы используем здесь, в отделе, — сказал он.

«Неясно, сработает ли это на самом деле. На бумаге это выглядит великолепно. С технической точки зрения это достижимо, по мнению поставщика облачных услуг, а также согласно нашему собственному анализу», — сказал МакКаун.

Неизвестно, выдержит ли он наступательные кибератаки, направленные на доступ к сети. Результаты испытаний будут иметь ключевое значение, «чтобы увидеть, сможем ли мы на самом деле получить эффект нулевого доверия, который мы хотим получить из этих облаков», — сказал журналистам Рэнди Резник, директор офиса нулевого доверия Министерства обороны США». ***(Lauren C. Williams. It's Finally Here: Pentagon Releases Plan To Keep Hackers Out Of Its Networks // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/its-finally-here-pentagon-releases-plan-keep-hackers-out-its-networks/380157/). 23.11.2022).***

***

«Министерство обороны согласовало инициативы и возможности в рамках Стратегии национальной обороны для обеспечения комплексного сдерживания.

Чтобы оставаться конкурентоспособным в киберпространстве по сравнению с государственными субъектами, такими как Китай и Россия, Агентство оборонных информационных систем должно продолжать налаживать прочные партнерские отношения для ускорения и внедрения технологий следующего поколения и инновационных решений для истребителей, заявил в понедельник главный офицер агентства.

«Наша основная цель в DISA — поддерживать американских военных, предоставляя бойцам нужную информацию, когда они в ней нуждаются», — сказал генерал-лейтенант ВВС Роберт Дж. Скиннер, директор DISA и штаб-квартира объединенных сил Министерства обороны. Сетевой командир.

«Это означает интеграцию различных программ для обеспечения связи между штаб-квартирой DISA и передовой», — добавил Скиннер во время конференции DISA Forecast to Industry 2022 в Таусоне, штат Мэриленд.

Министерство обороны согласовало инициативы и возможности в рамках Стратегии национальной обороны для поддержания комплексного сдерживания против государственных субъектов и других угроз, сказал Джон Шерман, директор по информационным технологиям Министерства обороны США». ***(Partnerships Necessary to Bolster DISA, DOD CIO Zero Trust, JADC2 Priorities // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/partnerships-necessary-to-bolster-disa-dod-cio-zero-trust-jadc2-priorities/). 11.11.2022).***

***

«Серия «Защита цепочки поставок программного обеспечения» является результатом Enduring Security Framework (ESF) — межотраслевой рабочей группы государственного и частного секторов, возглавляемой АНБ и CISA.

Сегодня CISA, Агентство национальной безопасности (АНБ) и Управление директора национальной разведки (ODNI) опубликовали третью часть серии из трех статей по обеспечению безопасности цепочки поставок программного обеспечения: Серия «Безопасность цепочки поставок программного обеспечения — Руководство по рекомендуемым практикам». для клиентов. Эта публикация следует за выпуском руководства для разработчиков за август 2022 г. и выпуском руководства для поставщиков за октябрь 2022 г.

Опубликованное сегодня руководство вместе с сопроводительным информационным бюллетенем содержит рекомендуемые методы для клиентов программного обеспечения для обеспечения целостности и безопасности программного обеспечения на этапах закупки и развертывания.

Серия «Защита цепочки поставок программного обеспечения» является результатом Enduring Security Framework (ESF) — межотраслевой рабочей группы государственного и частного секторов, возглавляемой АНБ и CISA. Эта серия дополняет другие усилия правительства США, направленные на то, чтобы помочь экосистеме программного обеспечения защитить цепочку поставок, такие как сообщество разработчиков программного обеспечения (SBOM).

CISA рекомендует всем организациям, участвующим в цепочке поставок программного обеспечения, ознакомиться с этим руководством. Дополнительную информацию см. на веб-страницах Целевой группы по управлению рисками цепочки поставок информационных и коммуникационных технологий (ИКТ) CISA, Библиотеке ресурсов цепочки поставок ИКТ и на веб-страницах Национального центра управления рисками (NRMC)». ***(CISA, NSA, and ODNI Release Guidance for Customers on Securing the Software Supply Chain // Homeland Security Today (https://www.hstoday.us/federal-pages/dhs/cisa-nsa-and-odni-release-guidance-for-customers-on-securing-the-software-supply-chain/). 18.11.2022).***

***

«…Канада объявила о своей стратегии в Индо-Тихоокеанском регионе 27 ноября, начиная с инвестиций в размере почти 2,3 миллиарда канадских долларов в течение следующих пяти лет.

В регионе находится множество горячих точек безопасности с потенциальными глобальными последствиями, и стратегия Канады предусматривает участие Канады в качестве регионального партнера по безопасности для защиты своих национальных интересов и безопасности…

Для продвижения интересов мира и безопасности в регионе Канада инвестирует более 720 миллионов долларов. Это включает 492,9 миллиона долларов на усиление военно-морского присутствия Канады в Индо-Тихоокеанском регионе и расширение участия канадских вооруженных сил в региональных военных учениях; и 47,3 млн долларов на запуск новой многоведомственной инициативы, направленной на развитие потенциала кибербезопасности у отдельных региональных партнеров. Канадское правительство также увеличит ресурсы, выделяемые на защиту канадцев от попыток иностранных государств тайно или принудительно повлиять на них.

В стратегии говорится, что Канада будет работать с союзниками для повышения осведомленности о регионе и повышения устойчивости и готовности, а также для защиты от тактики принуждения и кражи конфиденциальных данных, технологий и интеллектуальной собственности у компаний и исследовательских организаций. Кроме того, в стратегии отмечается, что влияние изменения климата на безопасность усиливает необходимость работы с региональными партнерами для повышения устойчивости к стихийным бедствиям, связанным с изменением климата. «Военные Канады будут работать со своими коллегами и обмениваться передовым опытом для повышения устойчивости к стихийным бедствиям, связанным с изменением климата», — говорится в документе.

Как арктическая нация, Канада осознает, что державы Индо-Тихоокеанского региона смотрят на Арктику как на регион возможностей. «Канада привержена делу поддержания мира и стабильности в регионе, а также безопасности, здоровья и устойчивости канадского северного населения и коренных народов», — говорится в стратегии. «Во время ускоряющегося воздействия изменения климата и растущей геополитической конкуренции Канада будет укреплять свои позиции в качестве арктической державы и поддерживать наш арктический суверенитет и основанный на правилах международный порядок в нашем двустороннем и многостороннем взаимодействии со странами Индо-Тихоокеанского региона по арктическим и полярные дела».

Полную версию стратегии читайте в правительстве Канады». ***(Kylie Bielby. Canada’s New Indo-Pacific Strategy Includes Cybersecurity and Naval Defense Investment // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/climate-security/canadas-new-indo-pacific-strategy-includes-cybersecurity-and-naval-defense-investment/). 28.11.2022).***

***

«Депутатов предупредили, что они становятся мишенью «враждебных государств», а их мобильные телефоны являются «потенциальным кладезем» конфиденциальной информации.

В письме депутатам спикер Палаты общин сэр Линдси Хойл призвал депутатов не использовать свой телефон для деликатных разговоров и даже не держать его в одной комнате.

«Если хакеры включили микрофон на одном телефоне, все в комнате могут быть услышаны», — написал он.

Правительство создает оперативную группу для защиты Великобритании от враждебных акторов.

В прошлом месяце появились сообщения о том, что телефон бывшего премьер-министра Лиз Трасс был взломан, когда она была министром иностранных дел.

The Mail on Sunday сообщила, что личные сообщения между г-жой Трасс и иностранными официальными лицами, в том числе о войне на Украине, попали в иностранные руки.

Что касается письма, о котором впервые сообщило HuffPost UK, в офисе сэра Линдсея заявили, что в нем не обсуждаются вопросы безопасности.

Тем не менее, он был передан BBC депутатом, который его получил.

В нем сэр Линдсей сказал: «Как показали недавние события, враждебные государства продолжают преследовать парламентариев, чтобы получить представление о наших демократических процессах или оказать влияние на них для получения экономической, военной или политической выгоды».

Он предупредил, что ни один мобильный телефон нельзя сделать полностью безопасным, но поделился советом правительственного Национального центра кибербезопасности, чтобы свести к минимуму риск компрометации телефона.

Совет включает в себя ограничение времени, в течение которого сообщения сохраняются на устройстве, и ограничение доступа к микрофонам и службам определения местоположения.

Один депутат сказал Би-би-си, что предупреждение было необходимо, потому что «мы безнадежно слабы» в отношении информационной безопасности.

Другой назвал этот совет «совершенным здравым смыслом», добавив: «Я уверен, что за нами постоянно наблюдают государственные деятели».

Письмо было опубликовано после того, как ранее в этом месяце правительство объявило о создании специальной рабочей группы для защиты «демократической целостности» Великобритании перед лицом угроз со стороны враждебно настроенных субъектов.

Министр безопасности Том Тугендхат сказал, что целевая группа рассмотрит самые разные вопросы, от физических угроз депутатам до кибербезопасности.

Правительственный законопроект о национальной безопасности, который содержит меры, направленные на борьбу с такими угрозами, как шпионаж, экономический шпионаж, иностранное вмешательство и саботаж, в настоящее время проходит через парламент.

Законопроект направлен на то, чтобы объявить преступлением вмешательство в британскую демократию и гражданское общество путем дезинформации или нападок на ее избирательные процессы.

Новая схема регистрации иностранного влияния будет направлена на то, чтобы заставить любого, кто действует от имени иностранной державы или организации, заявлять о любой деятельности по оказанию политического влияния, которую они

осуществляют». ***(Damian Grammaticas. Hostile states are targeting you, Speaker warns MPs // BBC (https://www.bbc.com/news/uk-politics-63654863). 16.11.2022).***

***

«Сайт Європарламенту зазнав кібератаки після того, як інституція визнала Росію державою-спонсором тероризму. Відповідальність за атаку взяли на себе прокремлівські хакери.

«Сайт Європарламенту зазнає складної кібератаки. Прокремлівське угруповання взяло на себе відповідальність», – повідомила президентка Європарламенту Роберта Мецола.

Мецола додала, що профільні IT-експерти протистоять атаці та захищають системи.

«Це сталося після того, як ми визнали Росію державою-спонсором тероризму. Моя відповідь: Слава Україні!», – підкреслила Мецола.

«Наразі доступність веб-сайту Європарламенту порушена через високий рівень зовнішнього мережевого трафіку. Цей трафік пов'язаний із DDOS-атакою», – повідомив речник Європарламенту Жауме Дуч.

Дуч додав, що фахівці працюють над «якнайшвидшим усуненням цієї проблеми»…». ***(Російські хакери атакували сайт Європарламенту після визнання РФ спонсором тероризму // ДМ media sapiens (https://ms.detector.media/kiberbezpeka/post/30723/2022-11-23-rosiyski-khakery-atakuvaly-sayt-ievroparlamentu-pislya-vyznannya-rf-sponsorom-teroryzmu/). 23.11.2022.)***

***

«Злам сторінок у соцмережах і оприлюднення «листування» перших осіб держави збігся у часі з активізацією проросійських протестів у Молдові.

Служба інформації та безпеки Молдови вважає, що витік «інформації» з телеграм-каналів перших осіб держави був справою рук спецслужб інших країн, а головними підозрюваними є росіяни.

Як повідомляє «Європейська правда» з посиланням на Newsmaker, ще 9 листопада невідомі зламали офіційні телеграм-канали президентки Молдови Маї Санду та віце-прем’єра Андрея Спину. На обох каналах з’явилися ідентичні повідомлення, начебто головними корупціонерами у Молдові є ті, хто з нею має боротися, і вся правда – «у прокуратурі та міністерстві юстиції».

Наступного дня, 11 листопада, хакери розмістили в інтернеті нібито фрагменти листування в телеграмі міністра юстиції Молдови Серджу Литвиненка й радника президентки Маї Санду Доріна Речана.

Цей злам стався на тлі активізації антиурядових протестів у Молдові проросійської Партії соціалістів екс-президента Ігоря Додона і популістської партії «Шор», яка, за деякими оцінками, конкурує з ними за роль «головного союзника» Росії у Молдові. Нещодавно уряд країни подав запит до Конституційного суду щодо визнання партії «Шор» незаконною через її фінансування коштами незрозумілого походження.

«Складається враження, що це (злам соцмереж та витік «листування», – ред.) скоординована акція, яка має на меті створити певний розбрат, напругу в суспільстві, спробувати підірвати довіру громадян до державних інституцій. Це було зроблено у напрочуд вдало обраний день, коли уряд схвалив і направив до Конституційного суду досить важливий запит – перевірку конституційності цієї партії («Шор» – ред.)», – заявив керівник Служби інформації та безпеки Александр Мустяца в етері телеканалу Pro TV в понеділок.

Мустяца додав, що характер поширення «зливу» в певних Telegram-каналах та ЗМІ може свідчити про спеціальну операцію з дискредитації. «За попереднім аналізом, за цими діями, схоже, стоять спецслужби інших держав», – зазначив він, уточнивши, що спецслужби Російської Федерації є «головними підозрюваними».

Мустяца заявив, що сумнівається в правдивості листування, яке опублікували невідомі хакери, адже «маючи доступ до Telegram-акаунту, можна створювати повідомлення, і важко довести, що є правдою, а що – ні»…» ***(Молдова підозрює спецслужби РФ у зламі телеграм-каналів президентки та міністрів // ДМ media sapiens (https://ms.detector.media/kiberbezpeka/post/30667/2022-11-15-moldova-pidozryuie-spetssluzhby-rf-u-zlami-telegram-kanaliv-prezydentky-ta-ministriv/). 15.11.2022.)***

***

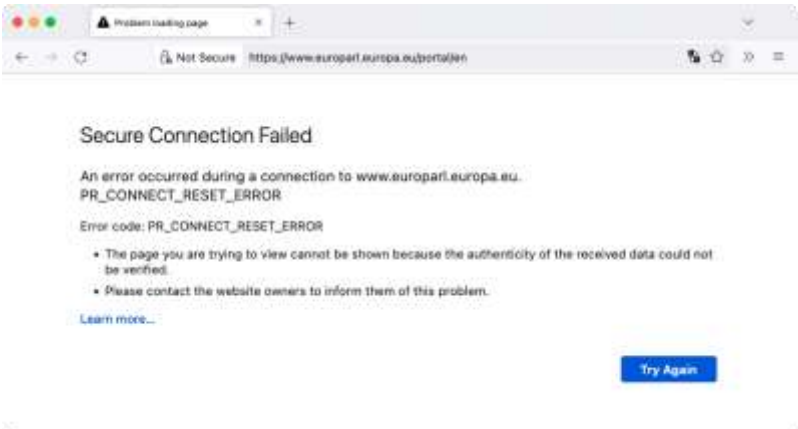
«Сайт Европарламента был закрыт после DDoS-атаки (распределенного отказа в обслуживании), за которую взялась пророссийская группа хактивистов, называющих себя Anonymous Russia.

Президент Европейского парламента подтвердил инцидент, заявив, что «парламентские ИТ-эксперты сопротивляются этому и защищают наши системы».

Генеральный директор по коммуникациям и пресс-секретарь Европейского парламента Жауме Даух также заявил после того, как сайт вышел из строя, что сбой был вызван продолжающейся DDoS-атакой.

«На доступность веб-сайта Europarl_EN в настоящее время влияет извне из-за высокого уровня внешнего сетевого трафика», — сказал Дауче.

«Этот трафик связан с событием DDOS-атаки (распределенный отказ в обслуживании). Команды ЕР работают над тем, чтобы решить эту проблему как можно быстрее».



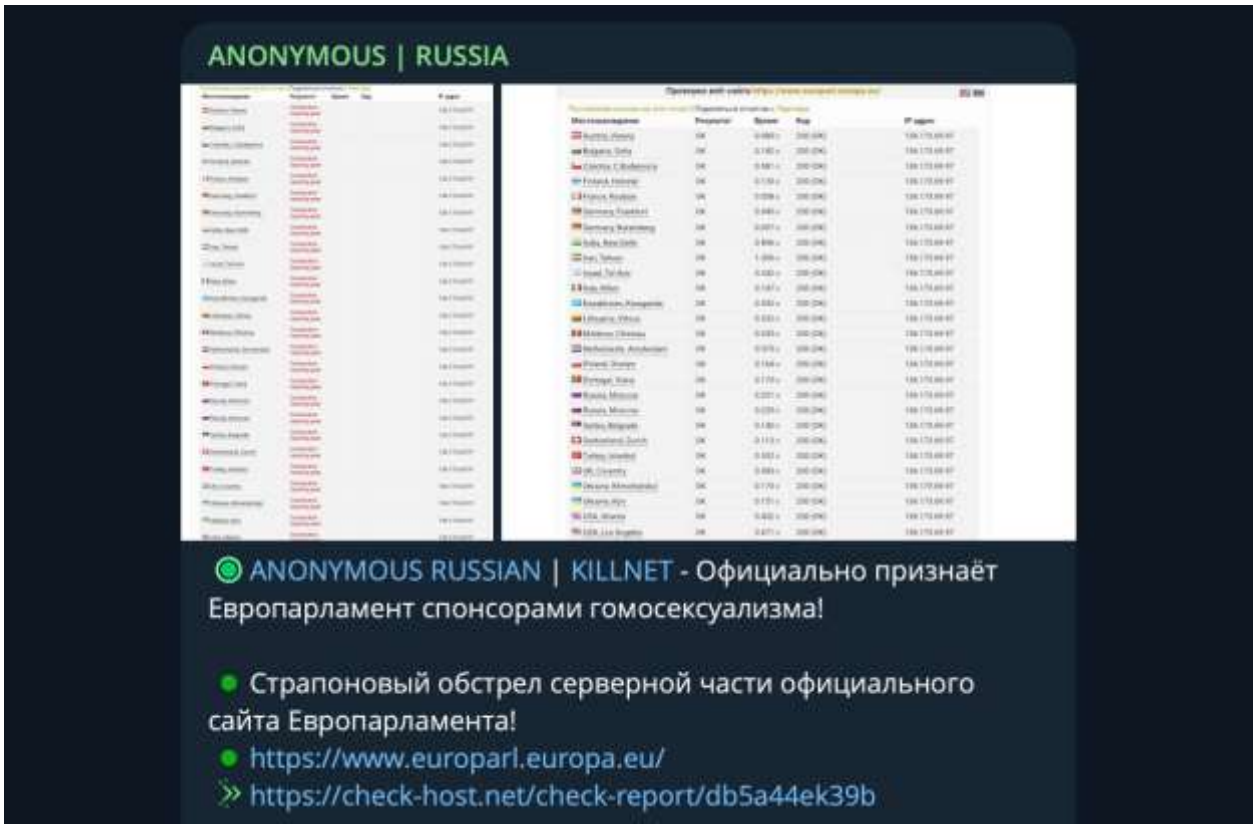
Сайт Европарламента не работает (BleepingComputer)

Атака произошла после того, как Европарламент признал Россию государством-спонсором терроризма, а депутаты Европарламента призвали к дальнейшей международной изоляции России.

Резолюция была принята в среду после недавних событий в агрессивной войне России против Украины.

«Парламент призывает Европейский Союз к дальнейшей международной изоляции России, в том числе в том, что касается членства России в международных организациях и органах, таких как Совет Безопасности ООН», — говорится в опубликованном сегодня пресс-релизе.

«Депутаты Европарламента также хотят, чтобы дипломатические отношения с Россией были сокращены, контакты ЕС с официальными российскими представителями были сведены к абсолютному минимуму, а связанные с Россией государственные учреждения в ЕС, распространяющие пропаганду по всему миру, были закрыты и запрещены».



Anonymous Russia заявляет об атаке на Европарламент (BleepingComputer)

Группы прокремлевских хактивистов атаковали европейские и американские веб-сайты с тех пор, как Россия вторглась в Украину. Например, Killnet недавно заявила о крупномасштабных распределенных атаках типа «отказ в обслуживании» (DDoS), нацеленных на веб-сайты нескольких крупных аэропортов США в прошлом месяце.

Известные примеры того, как веб-сайты аэропортов были закрыты после их атаки, включают международный аэропорт Лос-Анджелеса (LAX), который периодически отключался, и международный аэропорт Хартсфилд-Джексон в Атланте (ATL), крупный узел воздушного движения США.

За неделю до этого они с умеренным успехом атаковали несколько правительственных веб-сайтов США в Колорадо, Кентукки и Миссисипи, сумев на короткое время отключить некоторые из них.

Killnet также заявила, что закрыла веб-сайт системы управления информацией о защищенной критической инфраструктуре CISA после того, как ее атаки на Министерство финансов США в начале октября были предотвращены, прежде чем они оказали реальное влияние на инфраструктуру агентства.

Они также ранее нацеливались на страны, которые встали на сторону Украины, включая Румынию и Италию, в то время как «подгруппа» Легиона атаковала ключевые норвежские и литовские организации по тем же причинам.

Ранее в этом месяце ФБР заявило, что DDoS-атаки, координируемые пророссийскими хактивистами, оказывают незначительное влияние на их цели, поскольку они атакуют общедоступную инфраструктуру, такую как веб-сайты, а не сами сервисы, что приводит к ограниченным нарушениям». ***(Sergiu Gatlan. Pro-Russian hacktivists take down EU Parliament site in DDoS attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/pro-russian-hacktivists-take-down-eu-parliament-site-in-ddos-attack/). 23.11.2022).***

***

«Meta удалила несколько учетных записей в Facebook и Instagram, связанных с вооруженными силами США, заявив, что они использовались в рамках тайных операций влияния, направленных на Ближний Восток и Россию.

Meta заявляет, что удалила 39 учетных записей Facebook, 26 учетных записей Instagram, 16 страниц Facebook и две группы Facebook за нарушение политики «скоординированного недостоверного поведения».

У самой успешной из этих страниц Facebook было 22 000 подписчиков; более обширная группа насчитывала 400 участников, а у одного из заблокированных аккаунтов в Instagram было 12 000 подписчиков.

«Сеть США, связанная с лицами, связанными с вооруженными силами США, работала во многих интернет-сервисах и была сосредоточена на Афганистане, Алжире, Иране, Ираке, Казахстане, Кыргызстане, России, Сомали, Сирии, Таджикистане, Узбекистане и Йемене», — говорится в сообщении.

Meta обнаружила недостоверные аккаунты после того, как было начато внутреннее расследование на основании информации независимых исследователей из Graphika и Стэнфордской интернет-обсерватории, которые в августе 2022 года опубликовали пятилетний обзор тайных операций прозападного влияния.

Сеть дезинформации работала в кластерах, которые продвигали конкретные темы, соответствующие интересу аудитории из упомянутых стран.

Плакаты притворялись местными жителями этих стран, используя поддельные фотографии, созданные инструментами GAN (генеративно-состязательной сети), чтобы избежать разоблачения путем обратного поиска изображений.

Примечательно, что некоторые из заблокированных страниц использовали свои собственные уникальные логотипы и визуальный стиль и были связаны с

соответствующими учетными записями на YouTube, Twitter, Вконтакте и на специализированных веб-сайтах.

«Они публиковали видео, статьи, фотографии и мемы о стране, на которой сосредоточились. Когда эти бренды использовали одно и то же изображение или мем, каждый из них накладывал на него свой собственный логотип, что, вероятно, делало контент более уникальным и достоверным». - Мета

Признаком того, что это были поддельные учетные записи, было то, что они размещались в рабочее время США, а не в часовых поясах стран, в которых они предположительно базировались.

Люди, стоящие за этими кластерами, размещали посты на арабском, фарси и русском языках, чтобы восхвалять американских вооруженных сил и поднимать обеспокоенность по поводу терроризма в регионах, представляющих особый интерес.

Поддельные аккаунты потратили 2500 долларов на рекламу в Facebook, чтобы их дезинформационный контент достиг большего числа пользователей.

Во многих случаях кампании критиковали Иран, Китай и Россию, уделяя особое внимание российскому вторжению в Украину, угнетению Китаем уйгурского народа, поддержке двумя странами режима талибов в Афганистане и влиянию Ирана на Ближнем Востоке…». ***(Bill Toulas. Meta links U.S. military with covert Facebook influence operation // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/meta-links-us-military-with-covert-facebook-influence-operation/). 23.11.2022).***

***

«Правительство США через Федеральную комиссию по связи (FCC) запретило продажу оборудования китайских поставщиков телекоммуникаций и видеонаблюдения Huawei, ZTE, Hytera, Hikvision и Dahua из-за «неприемлемых рисков для национальной безопасности».

«Федеральная комиссия по связи приняла новые правила, запрещающие разрешать ввоз или продажу в США коммуникационного оборудования, которое считается представляющим неприемлемый риск для национальной безопасности», — говорится в пресс-релизе Федеральной комиссии по связи.

«Эти новые правила являются важной частью наших текущих действий по защите американского народа от угроз национальной безопасности, связанных с телекоммуникациями», — прокомментировала председатель Дж. Розенворсел.

Запрет США распространяется не только на материнские компании, но и на их дочерние и зависимые компании.

«Новые правила запрещают авторизацию оборудования в рамках процесса сертификации FCC и четко указывают, что такое оборудование не может быть авторизовано в рамках процесса декларации соответствия поставщика или импортировано или продано в соответствии с правилами, допускающими освобождение от авторизации оборудования». - ФКК

США ранее обвиняли производителя телекоммуникационного оборудования Huawei в краже интеллектуальной собственности, данных исследований и

разработок, а также в установке бэкдоров в свои продукты, которые потенциально позволили бы правительству Пекина проводить шпионские операции.

Телекоммуникационные технологии от Huawei (в частности, 5G) и ZTE были запрещены или исключены за последние годы во многих странах, включая Австралию, Новую Зеландию, Индию, Японию, США, Канаду, Румынию и Великобританию.

Четыре года назад некоторые члены Европейского союза также выразили обеспокоенность по поводу угроз безопасности, связанных с технологиями, предоставляемыми Huawei и ZTE, и исключили две компании из участия в торгах по различным проектам.

Тем не менее, Huawei не была запрещена во всей Европе, поскольку некоторые страны полагаются на компанию для основных компонентов для операторов связи, но несколько членов приняли закон, ограничивающий риски от китайских поставщиков телекоммуникационного оборудования.

Производитель камер наблюдения Dahua был добавлен в «Список организаций» Министерства торговли США в октябре 2019 года, но продажа его оборудования потребителям и частным американским компаниям не была запрещена.

В марте 2021 года FCC включила все пять компаний, которым теперь запрещено присутствие на рынке Соединенных Штатов, в свой список коммуникационного оборудования и услуг (Covered List), поскольку они были «сочтены представляющими неприемлемый риск для национальной безопасности Соединенных Штатов». государства или безопасность и защита граждан Соединенных Штатов».

Пометка их как таковая означает, что федеральные субсидии больше не могут использовать или покупать оборудование у этих компаний.

Все четыре члена FCC, имеющие разную политическую ориентацию, единогласно проголосовали за принятие новых мер против пяти китайских технологических компаний.

BleepingComputer обратился ко всем пяти компаниям за комментариями по поводу решения FCC, но не получил ответа до момента публикации.

В заявлении Hikvision для China Daily говорится, что решение FCC не повлияет на национальную безопасность США, но затронет малый бизнес, местные органы власти, школьные округа и отдельных потребителей, поскольку они понесут более высокие затраты на аналогичную технологию.

Обновление от 29 ноября — Dahua Technology USA отправила BleepingComputer следующий комментарий:

Dahua продолжает пересматривать приказ FCC, но, основываясь на нашем текущем анализе, мы считаем, что действия, предпринятые в приказе, выходят далеко за рамки уставных полномочий Комиссии и мало или совсем ничего не сделают для защиты национальной безопасности США.

Тем не менее, приказ Федеральной комиссии по связи США не затрагивает продукты, которые уже разрешены, и оставляет Dahua путь для получения разрешений на дополнительные продукты в будущем, при условии, что они не

предназначены для общественной безопасности, государственных учреждений, критической инфраструктуры или целей национальной безопасности.

Учитывая, что продукты Dahua в настоящее время не продаются для этих целей и не продаются в течение нескольких лет, мы достаточно уверены, что этот Заказ позволит нам продолжать обслуживать большинство наших клиентов в США в течение многих лет.

Обновление 2, 29 ноября. ZTE отправила BleepingComputer следующий комментарий:

ZTE категорически не согласна с недавним решением Федеральной комиссии по связи США и оценивает варианты защиты своих интересов.

ZTE предпринимала неоднократные попытки конструктивного взаимодействия с политиками США, чтобы понять любые возможные опасения по поводу продуктов, которые она сейчас продает в Соединенных Штатах.

Правительство Соединенных Штатов никогда не выявляло каких-либо конкретных, поддающихся решению проблем в отношении продуктов, которые ZTE продает в Соединенных Штатах, или случаев, когда продукты ZTE использовались для нарушения безопасности США или конфиденциальности потребителей.

В свете текущей рыночной конъюнктуры ZTE постепенно сворачивает свои бизнес-операции из США и сосредоточит свой дальнейший рост на других рынках.

В настоящее время операции ZTE в США составляют менее 1% от общего дохода компании. Решение FCC не окажет существенного влияния на бизнес-операции ZTE». ***(Bill Toulas. US bans sales of Huawei, Hikvision, ZTE, and Dahua equipment // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/us-bans-sales-of-huawei-hikvision-zte-and-dahua-equipment/). 28.11.2022).***

***

«Huawei Technologies Co. і ZTE Corp. було заборонено продавати електроніку в США регуляторами, які стверджують, що вони становлять загрозу безпеці, продовжуючи багаторічну спробу обмежити доступ китайських телекомунікаційних компаній до мереж США.

У розпорядженні Федеральної комісії зі зв’язку, опублікованому в п’ятницю, також названі постачальники підключених камер Hangzhou Hikvision Digital Technology Co. і Dahua Technology Co., а також виробник двостороннього радіозв’язку Hytera Communications Corp.

«FCC прагне захищати нашу національну безпеку, гарантуючи, що ненадійне комунікаційне обладнання не буде дозволено використовувати в межах наших кордонів, і ми продовжуємо цю роботу тут», — сказала голова Джессіка Розенворсел у прес-релізі. «Ці нові правила є важливою частиною наших постійних дій із захисту американського народу від загроз національній безпеці, пов’язаних із телекомунікаціями».

Під час голосування 4-0 FCC дійшла висновку, що продукти становлять загрозу безпеці даних. Попередні спроби обмежити доступ Китаю включають експортний контроль, щоб відключити ключове, складне обладнання та програмне забезпечення. Нещодавно офіційні особи США зважили обмеження на TikTok через

побоювання, що китайська влада може отримати доступ до даних користувачів США через додаток для обміну відео.

«Кульмінація дії»

«Це кульмінаційна дія», — сказав Клон Кітчен, старший науковий співробітник Американського інституту підприємництва у Вашингтоні, громадсько-політичного аналітичного центру. «Те, що було розпочато за Трампа, зараз виконується. Адміністрація Байдена продовжує закручувати гайки на цих компаніях, оскільки загроза не змінюється».

Huawei відмовилася від коментарів, а Hikvision не надала коментарів одразу після того, як з ними зв'язалися. Dahua, Hytera та ZTE не відповіли на електронні листи, надіслані в неробочий час у Китаї.

За словами американського чиновника на умовах анонімності, під час двосторонньої зустрічі між президентом США Джо Байденом і президентом Китаю Сі Цзіньпіном в Індонезії минулого тижня цей крок FCC, що насувається, не згадувався. Байден дійсно обговорював із Сі технологічні питання більш широко, і було ясно, що США продовжуватимуть вживати заходів для захисту своєї національної безпеки, сказав чиновник.

«Це смертний дзвін для всіх них за їхні операції в США», — сказав Конор Хілі, директор урядових досліджень дослідницької групи IPVM у Віфлеємі, штат Пенсільванія. «Вони не зможуть представити будь-які нові продукти в США».

Найбільш викривлені

Dahua і Hikvision постраждають найбільше, оскільки їхні камери широко використовуються, часто урядовими установами з багатьма засобами для моніторингу, сказав Хілі. Агентства, включаючи поліцію, також використовують портативні радіостанції Hytera, сказав він.

У своєму розпорядженні FCC також попросила прокоментувати, чи відкликати існуючий дозвіл на використання обладнання, сказав Розенворцел в онлайн-заяві.

За словами Хілі, торговці можуть застрягти зі спорядженням, продавати яке заборонено.

У 2018 році Конгрес проголосував за заборону федеральним агентствам купувати обладнання в п'яти компаній, названих FCC. Раніше агентство заявило, що компанії не мають права отримувати федеральні субсидії, а також заборонило китайським телефонним компаніям вести бізнес у США.

Указ, виданий у п'ятницю, вимагався відповідно до законопроекту, підписаного Байденом у листопаді 2021 року, повідомляє агентство». ***(Дмитро Сизов. США забороняють телекомунікаційне обладнання Huawei, ZTE через ризик безпеки даних // Internetua (https://internetua.com/ssha-zaboronyauat-telekomunikaciine-obladnannya-huawei-zte-cserez-rizik-bezpeki-danih). 26.11.2022).***

***

«У Департаменті державної інфосистеми Естонії повідомили про масштабну атаку прокремлівських хакерів на підприємства й відомства Естонії, Латвії, Польщі та України.

Про це повідомляє портал ERR.

Керівник відділу CERT-EE по роботі з кіберінцидентами Департаменту державної інфосистеми (RIA) Тину Таммер повідомив, що о 10:14 ранку в суботу вони виявили, що послуги п'яти естонських компаній почали працювати зі збоями. Серед них був і державний енергоконцерн Eesti Energia.

«Через атаки, крім сайту Eesti Energia, недоступні сайти, пов'язані з підприємством, такі як elektrilevi.ee і enefitgreen.ee. Кіберексперти CERT-EE перебувають у тісному контакті з представниками підприємства», - сказав Таммер.

Таммер сказав, що злочинці також націлилися на міністерство економіки і комунікацій, Банк Естонії та фонд EAS, а також на сайт однієї приватної компанії.

Він також зазначив, що ніколи не можна з абсолютною впевненістю сказати, хто стоїть за атаками, але наявна інформація дає змогу припустити, що це прокремлівські кіберзлочинці.

«Наскільки нам відомо, в цей самий час атаці піддалися компанії та установи в Латвії, Польщі та Україні. Цей список може бути не остаточним», - сказав Таммер». ***(Прокремлівські хакери здійснили масштабну атаку на підприємства країн Балтії та України // Internetua (https://internetua.com/prokremlivski-hakeri-zdiisnili-masshtabnu-ataku-na-pidpriyemstva-krayin-baltiyi-ta-ukrayini). 20.11.2022).***

***

«Заявление Китая о техническом превосходстве с помощью своей армии хакеров представляет собой самую большую угрозу для будущей кибербезопасности Великобритании, говорится во вчерашнем отчете.

Глава Национального центра кибербезопасности (NCSC) Линди Кэмерон заявила, что стремительное техническое развитие Китая и глобальный шпионаж угрожают нашей национальной безопасности.

Она высказалась после того, как вчера было объявлено о создании новой оперативной группы для защиты британских демократических институтов от иностранного вмешательства со стороны враждебных государств.

Министр безопасности Том Тугендхат сказал депутатам, что новый орган будет рассматривать как физические, так и онлайн-угрозы депутатам.

Развитие событий произошло после того, как на прошлой неделе выяснилось, что личный телефон Лиз Трасс был взломан агентами Москвы, когда она была министром иностранных дел.

Вчера ежегодный обзор NCSC предупредил об «острой» онлайн-угрозе для Великобритании, исходящей от враждебных государств, включая Китай, Россию, Иран и Северную Корею.

Мисс Кэмерон предположила, что Китай представляет наибольшую угрозу интересам Великобритании.

Она сказала: «Техническое развитие и эволюция Китая, вероятно, станут самым большим фактором, влияющим на кибербезопасность Великобритании в ближайшие годы».

В отчете NCSC содержится предупреждение: «Китайские киберсилы на сегодняшний день являются крупнейшими в мире.

«С момента прихода к власти почти десять лет назад президент Си руководил обширной реформой разведывательного и военного аппарата Китая, при этом

ключевым приоритетом является слияние военных и гражданских кибервозможностей.

«С тех пор Министерство государственной безопасности Китая (МГБ) стало активным и всепроникающим игроком в киберпространстве, проводя масштабную глобальную шпионскую кампанию для достижения политических, социально-экономических и стратегических целей».

В апреле директор ФБР Кристофер Рэй заявил, что у Китая «программа взлома больше, чем у любой другой крупной страны вместе взятой».

Ежегодный обзор организации по кибербезопасности, которая является частью GCHQ, также указал на угрозу кибератак со стороны России, если президент Путин изменит тактику в войне против Украины.

Перед вторжением босс GCHQ сэр Джереми Флеминг и мисс Кэмерон провели круглые столы с руководителями отечественных энергетических, коммунальных, пищевых, коммуникационных, транспортных и других основных поставщиков услуг, чтобы проинформировать их о рисках «российской киберагрессии», хотя опасения по поводу волна кибератак на Британию оказалась необоснованной.

В настоящее время Великобритания является третьей страной, наиболее уязвимой для кибератак, уступая только США и Украине.

Но в отчете NCSC содержится предупреждение о том, что теперь Россия может изменить тактику: «Хотя британские организации не испытали значительного кибер-воздействия в результате вторжения России в Украину, Россия продолжает представлять собой постоянную и активную угрозу Великобритании и ее интересам, поэтому NCSC продолжает советовать не расслабляться.

«В ответ на недавние неудачи, которые Россия испытала на поле боя в Украине, они могут изменить свой подход к киберпространству конфликта». В докладе содержится предупреждение о том, что угрозы, исходящие от враждебных государств, в будущем будут расти.

В ближайшие годы вредоносные и разрушительные киберинструменты будут доступны «более широкому кругу государственных и негосударственных субъектов» благодаря развитию «хакеров по найму», предлагающих индивидуальные услуги, и «растущему серому рынку» для кибербезопасности. инструменты За последний год предприятия и организации в Великобритании сообщили в NCSC о сотнях кибер-инцидентов, 63 из которых были достаточно значительными, чтобы потребовать реагирования на национальном уровне.

Среди них 18 инцидентов с программами-вымогателями, в том числе атаки на поставщика NHS 111 и компанию водоснабжения South Staffordshire Water.

Позднее в палате общин г-н Тугендхат вчера объявил, что возглавит новую рабочую группу по борьбе с угрозами демократическим институтам Великобритании.

Он сказал: «Передовые технологии, на разработку которых наши соперники потратили время и деньги, уравняли поле и сделали нас более уязвимыми.

«Великобритания на протяжении поколений находилась на переднем крае защиты свободы; наши агентства и предприятия десятилетиями сталкивались с реальностью этой опасности.

«Наш парламент и наша политика теперь ничем не отличаются, будь то министры или теневые министры в комитете или при руководстве кампанией, это касается каждой партии и каждого члена этой палаты». ***(REBECCA CAMBER. Chinese Government hackers are the biggest threat to UK's cyber security, official report reveals // Associated Newspapers Ltd (https://www.dailymail.co.uk/news/article-11378599/Chinese-Government-hackers-biggest-threat-UKs-cyber-security-official-report-reveals.html). 01.11.2022).***

***

«Национальное агентство кибербезопасности и информационной безопасности предупредило о повышенном риске DDoS-атак на Чехию и чешские организации. Во вторник на своем веб-сайте он сообщил, что зарегистрировал рост таких вредоносных действий, направленных на нарушение нормального трафика на веб-сайтах.

Агентство сообщило, что за последний месяц наблюдается заметный рост таких атак, которые происходят в контексте геополитической ситуации в Восточной Европе». ***(Ian Willoughby. Cyber security agency says attacks on Czechia up // Radio Prague International (https://english.radio.cz/cyber-security-agency-says-attacks-czechia-8765828). 01.11.2022).***

***

«Даниэль Тобок, генеральный директор CYPFER, объявил о назначении опытного лидера киберразведки г-на Кадира Левента управляющим партнером CYPFER, управляющим головным офисом в Великобритании, обслуживающим Великобританию и Европу.

«Великобритания и Европейский Союз находятся под атакой», — говорит Даниэль Тобок, генеральный директор CYPFER. «Геополитический сдвиг, вызванный российским вторжением в Украину, привел к преднамеренным несоответствиям в применении государствами-членами ЕС международного права, регулирующего киберпространство, и приверженности системе кибернорм Организации Объединенных Наций, которые не могут остаться незамеченными или неисправленными», — говорит Тобок. Именно здесь Левент вступает в должность главного руководителя отдела кибербезопасности и разведки в Великобритании и ЕС для CYPFER.

«Я рад присоединиться к руководству CYPFER», — говорит Левент. «Я всегда глубоко уважал и восхищался Даниэлем Тобоком и его командой по всему миру и с нетерпением жду возможности поделиться своим опытом и страстью к отрасли с предложениями CYPFER, но понимаю и уважаю стоящую перед нами задачу — восстановить отношения Великобритании и Европы с бизнесом. как обычно, вдохновляют кибератаки и тех, кто за ними стоит», — говорит Левент.

Левент начал свою карьеру в области кибербезопасности в качестве следователя цифровой судебной экспертизы в столичной полицейской службе. Оттуда он перешел в индустрию киберстрахования, где работал старшим специалистом по реагированию на инциденты в Лондоне. Г-н Левент продвигал свою карьеру на руководящих должностях, таких как управляющий директор и

главный операционный директор, на рынке технологий цифровой криминалистики и реагирования на инциденты, где он создал высокоэффективные международные группы киберреагирования и добился многократного превышения целей роста.

«Его (Левента) навыки уникальны и важны для нашей фирмы и клиентов при реагировании на киберинциденты», — говорит Даниэль Тобок, генеральный директор CYPFER. «Краткий и уверенный ответ требует сильного лидерства киберразведки, которое воплощает в себе способности к расследованию, аналитике и решению проблем, и Левент стал ведущей демонстрацией этих способностей», — говорит Тобок.

Левент известен в отрасли киберразведки и безопасности как эффективный коммуникатор, работавший с клиентами на всех уровнях, от MD до ИТ-команд, решая сложные технические проблемы для всех аудиторий по различным вопросам кибербезопасности.

«Мы с нетерпением ждем наших планов международной экспансии под руководством Левента. Я верю, что с архитектурой и лидерством CYPFER наши клиенты станут более непобедимыми и менее уязвимыми в постоянно растущем кибер-интеллектуальном мире», — заключает Тобок». ***(CYPFER Executes European Strategy in Response to Rising Cyber Security Attacks Across EU // Cision US Inc (https://www.prnewswire.com/news-releases/cypfer-executes-european-strategy-in-response-to-rising-cyber-security-attacks-across-eu-301665165.html). 01.11.2022).***

***

«В понедельник в Литве прошли общеевропейские учения по реагированию на киберинциденты и кризисы BlueOLEX 2022.

«Поскольку на этот раз мы организуем учения, мы разработали четвертое издание, чтобы еще больше способствовать совместной координации крупномасштабных киберинцидентов и кризисов», — сказал в пресс-релизе заместитель министра обороны Маргирис Абукявичюс.

Учения совместно организуют Министерство обороны Литвы, Чехия, председательствующая в Совете Европейского Союза, и Агентство Европейского Союза по кибербезопасности (ENISA).

Цель состояла в том, чтобы развивать деятельность Сети организаций связи по киберкризису (CyCLONe), в которую входят руководители по кибербезопасности и реагированию на кризисы из стран-членов ЕС, Европейской комиссии и ENISA.

CyCLONe была основана в 2020 году для повышения общего уровня ситуационной осведомленности и обмена информацией, а также для улучшения скоординированного реагирования в Европейском Союзе в случае крупномасштабного киберинцидента или кризиса». ***(Lithuania hosts EU-wide cyber security exercise // Lietuvos nacionalinis radijas ir televizija (https://www.lrt.lt/en/news-in-english/19/1815746/lithuania-hosts-eu-wide-cyber-security-exercise). 07.11.2022).***

***

«Иран представляет реальную угрозу кибербезопасности для Саудовской Аравии и других стран Персидского залива и может нанести удар по ключевым

отраслям, таким как телекоммуникации, нефть и газ, сообщает Al Arabiya English.

Согласно отчету, нефтяной гигант Саудовской Аравии Aramco был взломан в 2012 году в результате одной из крупнейших на сегодняшний день кибератак в мире. Ответственность за атаку, в результате которой было повреждено около 30 000 компьютеров с целью остановить добычу нефти и газа, взяла на себя группа под названием «Резающий меч справедливости».

«Они [Иран] рассматриваются на мировой арене как серьезная угроза высшего уровня», — сказал Al Arabiya English Брюс Шнайер, эксперт по безопасности и научный сотрудник Центра Беркмана-Кляйна по вопросам Интернета и общества Гарвардского университета. «Я бы отнесся к ним очень серьезно».

В отчете говорится, что базирующаяся в Дубае американская компания CrowdStrike в настоящее время отслеживает 20 групп в Иране, которые могут нацеливаться на регион для потенциального кибершпионажа или атак…». ***(Iran poses major cyber-security threat to Gulf // Ardi Associates Ltd (https://www.middleeastmonitor.com/20221104-iran-poses-major-cyber-security-threat-to-gulf/). 04.11.2022).***

***

«Европейская комиссия предложила в четверг два плана действий по устранению ухудшения ситуации с безопасностью после вторжения России в Украину, чтобы укрепить киберзащиту и позволить вооруженным силам быстрее и лучше перемещаться через границы.

Представитель ЕС заявил, что российские кибератаки на страны Европейского союза и их партнеров стали «тревожным звонком». В нем говорится, что необходимы дополнительные действия для защиты граждан и вооруженных сил, а также необходимо активизировать сотрудничество с НАТО.

«Война вернулась к нашим границам, а агрессия России против Украины подрывает мир и международную правовую систему во всем мире», — заявил на пресс-конференции глава внешнеполитического ведомства ЕС Жозеп Боррель, объявив о планах.

«Это влияет на нас, и мы должны адаптировать нашу оборонную политику к этой новой среде».

Отдельно генеральный секретарь НАТО Йенс Столтенберг предупредил о растущих угрозах в киберпространстве, отметив недавние атаки на спутники, критически важную инфраструктуру и правительственные учреждения, особенно в рамках войны России против Украины.

«Кибер — это постоянно оспариваемое пространство, и грань между миром, кризисом и конфликтом размыта», — заявил глава возглавляемого США оборонного альянса в своем выступлении в Риме.

«Я призываю союзников подтвердить приверженность киберзащите. С большими деньгами, большим опытом и расширенным сотрудничеством. Это жизненно важная часть нашей коллективной защиты, и мы все вместе».

ВОЗМОЖНОСТИ

Политика, предложенная Европейской комиссией, повысит возможности киберзащиты ЕС и укрепит координацию и сотрудничество между военными и гражданскими киберсообществами.

Эта инициатива является частью ряда мер, предложенных Комиссией по укреплению кибербезопасности ЕС на фоне волны кибератак на правительства и предприятия по всему миру.

На прошлой неделе агентство ЕС по кибербезопасности ENISA заявило, что вторжение в Украину привело к более разрушительным и широкомасштабным кибератакам в ЕС с начала года до июля.

Отдельный План действий по военной мобильности, предложенный Комиссией, направлен на то, чтобы помочь странам ЕС и их партнерам более эффективно перевозить войска и технику, работать над «лучше связанной и защищенной инфраструктурой» и укреплять сотрудничество с НАТО.

«…чтобы вооруженные силы могли реально что-то изменить на местах, они должны двигаться быстро. Их нельзя блокировать из-за бюрократии или отсутствия адаптированной инфраструктуры», — заявила на пресс-конференции в четверг вице-президент Еврокомиссии Маргрет Вестагер». ***(John Chalmers. EU proposes cyber defence plan as concerns about Russia mount // Reuters (https://www.reuters.com/world/europe/eu-proposes-cyber-armed-forces-plans-amid-security-concerns-2022-11-10/?rpc=401&). 10.11.2022).***

***

«Китай призывает Соединенные Штаты прекратить безответственные обвинения других стран в кибербезопасности, заявил в среду официальный представитель министерства иностранных дел.

Пресс-секретарь Мао Нин сделал это заявление на регулярном брифинге для прессы, отвечая на вопрос о заявлениях о том, что разведывательное сообщество США начало попытки помешать шпионам и хакерам из Китая и других стран получить доступ к академическим исследованиям по новым технологиям.

Она сказала, что китайское правительство всегда было категорически против хакерских атак и злоупотребления информационными технологиями.

Отметив, что Соединенные Штаты являются страной, обладающей самыми мощными кибертехнологиями и возможностями в мире, Мао сказал, что Соединенные Штаты также предприняли наибольшее количество хакерских атак, прослушивания телефонных разговоров и тайных краж в отношении других стран.

«Недавний отчет показывает, что США предприняли кибератаки и операции по краже против Северо-Западного политехнического университета Китая и забрали группу основных технических данных. Но США еще не предложили объяснения», — сказала она, призвав Соединенные Штаты немедленно остановить кибератаки и тайные кражи против других стран, а также прекратить выдвигать безответственные обвинения против других в отношении кибербезопасности». ***(China urges US to stop irresponsible accusations on cyber security // China.org.cn (http://www.china.org.cn/world/2022-11/17/content_78523364.htm). 17.11.2022).***

***

«Рост стоимости утечек данных, программ-вымогателей и других кибератак приводит к росту взносов на киберстрахование и более ограниченному покрытию киберстрахования. Эта ситуация с киберстрахованием увеличивает риски для организаций, пытающихся найти покрытие или сталкивающихся с резким увеличением.

Некоторые клиенты юридической фирмы Akin Gump Strauss Hauer & Feld LLP, например, сообщили о трехкратном увеличении страховых тарифов, а перевозчики «огромно снижают» лимиты покрытия за последние два года. Соруководитель их практики кибербезопасности Мишель Рид добавляет: «Сниженная сумма покрытия больше не может защитить страхователей от киберубытков. Полис на 10 миллионов долларов может закончиться ограничением в 150 000 долларов на кибермошенничество».

Ситуация с киберстрахованием настолько тревожна, что министерство финансов США недавно опубликовало запрос на общественное мнение о потенциальной федеральной программе реагирования на киберстрахование. Этот запрос является дополнением к оценке, проведенной совместно Федеральным страховым управлением (FIO) и Агентством кибербезопасности и безопасности инфраструктуры (CISA) Министерства внутренней безопасности для определения «степени, в которой риски для критически важной инфраструктуры от катастрофических киберинцидентов и потенциальных финансовых воздействия требуют федерального страхового ответа».

Это прямой результат эволюции характера кибератак, отражающей эволюцию цифровых сред и эффект облегчения преступлений с помощью криптовалюты. Что касается киберпреступников, то самодельные комплекты вредоносных программ и платформы «Вредоносное ПО как услуга» устранили входной барьер для киберпреступников и сделали запуск сложных атак доступным для подражателей-преступников, которым не хватает технических знаний.

Покрытие киберстрахования раньше покрывало только прерывание бизнеса, восстановление данных и ущерб инфраструктуре. Сегодня они также должны покрывать расходы на кибер-вымогательство, репутационные риски, штрафы за несоблюдение требований и риски ответственности перед третьими лицами, что является растущей областью, поскольку взаимосвязь между организациями продолжает расширяться.

Классическими инструментами оценки премиум-класса страховщика киберстрахования являются оценка соблюдения лучших практик и тестирование на проникновение. Однако ограничения, присущие этим подходам, проблематичны на многих уровнях.

Ограничения оценки на основе передового опыта:

Не все лучшие практики подходят для каждой организации.

Даже соблюдение лучших практик обеспечивает ограниченную защиту.

Некоторые передовые методы, такие как комплексное исправление, недостижимы. Даже ограничение исправления уязвимостями с оценкой CVSS выше

9 нереально. Из 20184 новых уязвимостей, обнаруженных в 2021 году, 1165 получили оценку выше 9.

Ограничения тестирования на проникновение

Достоверность результатов зависит от способностей тестировщика и инструментов.

Ему не хватает непрерывности. В качестве точечного теста он предоставляет снимок организации в определенный момент времени: гибкая разработка, возникающие угрозы и взаимосвязанность ограничивают релевантность тестирования на проникновение в течение всего срока службы.

Методы непрерывной проверки безопасности, такие как моделирование взлома и атаки, управление поверхностью атаки и оценка воздействия угроз, которые оптимизируют программы безопасности, минимизируют воздействие и предоставляют количественные ключевые показатели эффективности, которые можно отслеживать с течением времени, меняют правила игры. Переход от защитной, реактивной точки зрения к оценке подверженности застрахованной стороне угрозе подразумевает переход к оценке фактического ущерба, который могут нанести атаки по всей матрице MITRE ATT&CK TTP.

При переговорах с страховщиком киберстрахования компания, которая может предоставить количественные, документированные оценки, выполненные с использованием технологий проверки безопасности, может возглавить обсуждение, продемонстрировав, как она:

Снижает риски сверх лучших практик. Всесторонние оценки измеряют уровень безопасности организации на основе ее фактической устойчивости к атакам, а не теоретического прогноза безопасности, полученного за счет соблюдения передовых практик.

Количественная оценка риска. Количественные оценки риска, основанные на проценте эмуляции атаки, обнаруженной и предотвращенной набором средств защиты, обеспечивают мгновенную оценку фактической эффективности киберзащиты. Усовершенствованные технологии проверки безопасности включают полную оценку цепи уничтожения и возможности бокового перемещения, которые обеспечивают точную оценку степени потенциального ущерба, который может быть нанесен в результате успешного взлома.

Предотвращает дрейф системы безопасности. Поскольку автоматизация моделирования атак обеспечивает непрерывную переоценку устойчивости в контексте, бреши в безопасности, возникающие в результате новых развертываний или возникающих угроз, сразу же помечаются и могут быть устранены до того, как возникнет угроза безопасности.

Открывает новые возможности андеррайтинга в сфере киберстрахования. Непрерывный характер проверки безопасности можно использовать для определения этапов политики после связывания. Предлагая непрерывную или периодическую переоценку состояния безопасности, определяемую оценкой безопасности, для измерения эволюции состояния безопасности с течением времени, предоставляет застрахованной стороне действенные средства ведения переговоров.

Договор страхования может включать такие элементы, как требования об устранении отклонений от согласованных исходных условий в разумные сроки,

обязательство регулярно обмениваться автоматически формируемыми отчетами об оценке или связь между степенью покрытия и соблюдением исходных отклонений.

Подтверждение безопасности становится способом соблюдения нормативных требований, как, например, недавнее обновление PCI DSS v4.0. Включение проверки безопасности в процессы андеррайтинга киберстрахования может иметь большое значение для решения текущей ситуации с киберстрахованием и повышения киберустойчивости организаций, у которых будет дополнительный стимул для внедрения такого упреждающего подхода в своей среде». ***(Andrew Barnett. Re-Focusing Cyber Insurance with Security Validation // The Hacker News (https://thehackernews.com/2022/11/re-focusing-cyber-insurance-with.html). 10.11.2022).***

***

«Страховые компании настаивают на помощи налогоплательщиков для обеспечения покрытия в случае катастрофических происшествий.

Министерство финансов и Агентство по кибербезопасности и безопасности инфраструктуры продлили свой первоначальный крайний срок — с понедельника — до 14 декабря для получения комментариев общественности о том, следует ли использовать федеральные средства для обеспечения защиты критически важной инфраструктуры от убытков от кибератак, и если да, то как может быть разработана федеральная программа страхования.

Агентства объявили о продлении в уведомлении от 9 ноября, опубликованном в Федеральном реестре.

В соответствии с рекомендацией Счетной палаты правительства по указанию Конгресса расследовать этот вопрос, агентства ищут ответы о том, «в какой степени риски для критически важной инфраструктуры от катастрофических кибер-инцидентов и потенциальных финансовых рисков требуют ответных действий федерального страхования». к уведомлению.

Возвращаясь к администрации Обамы, киберстрахование рассматривалось политиками всего политического спектра как нерегулируемый способ стимулирования соответствующих методов кибербезопасности со стороны организаций частного сектора. Запрос агентств о комментариях поступил в связи с рядом событий последних лет, в том числе решениями по ключевым судебным делам, и совпал с тем, что страховые компании призывают к федеральной программе страхования от киберугроз.

В декабре 2019 года Конгресс принял закон об ассигнованиях, предписывающий GAO сообщать о наличии киберстрахования для поставщиков критической инфраструктуры. В мае 2021 года GAO сообщило о проблемах, стоящих перед отраслью, которые, по словам наблюдательного органа, можно решить. А в июне GAO поручило Министерству финансов и CISA провести дальнейшее расследование необходимости федеральной программы, аналогичной Национальной программе страхования от наводнений, проводимой Федеральным агентством по чрезвычайным ситуациям, или Федеральной программе страхования урожая при Министерстве сельского хозяйства.

В своем первоначальном запросе комментариев от 29 сентября Министерство финансов и CISA заявили, что они также рассмотрят вопрос о том, как Программа страхования от террористических рисков, или TRIP, может быть адаптирована для покрытия инцидентов кибербезопасности, но что их внимание будет сосредоточено в первую очередь на подходах, не связанных с TRIP, в домашних условиях. или за границей.

Модель TRIP, созданная после террористических атак 11 сентября, по существу обеспечивает страхование страховщиков, помогая им страховать держателей полисов в случае соответствующих инцидентов. Но существует ограничение в 100 миллиардов долларов на сумму, которую правительство может выплатить, и в уведомлении агентств цитируется исследование CISA, опубликованное в 2020 году, в котором потенциальные убытки от одного кибер-инцидента оцениваются в диапазоне от 2,8 миллиардов долларов до 1 триллиона долларов. И соблюдение критериев террористической атаки может оказаться сложной задачей для тех, кто ищет защиту после инцидента с кибербезопасностью.

Федеральные страховые программы, как правило, создаются для того, чтобы страхователи покрывали убытки во время непредвиденных стихийных бедствий — так называемых «стихийных бедствий», — которые приводят к множеству претензий сразу, полностью превышая способность страховщиков выполнять свои обязательства.

Возможность кибератак вызвать каскадные последствия и увеличить количество страховых требований от страхователей полностью проявилась во время атаки NotPetya в 2017 году, которая началась в Украине, но оказала огромное влияние на американские компании.

В двух крупных случаях страховые компании отказались покрывать претензии, сославшись на исключения «военных действий» из-за участия государственного актора. Официальные лица США приписывают атаку NotPetya России, но в решении от 13 января суд Нью-Джерси постановил, что страховая компания Ace не предоставила достаточного уведомления о том, как исключение будет применяться в полисе страхования имущества судоходной компании Merck на сумму 1,7 миллиарда долларов.

Сообщается, что дело Merck находится на рассмотрении апелляции от Ace, которая, по словам суда, должна выплатить 1,4 миллиарда долларов США по иску Merck в качестве компенсации компьютерного ущерба. Совсем недавно The Record сообщила, что страховая компания Zurich урегулировала судебный процесс на 100 миллионов долларов с гигантом по производству закусок Mondelez после того, как первоначально отказалась оплатить иск последнего, связанный с NotPetya, учитывая акт об исключении из войны.

Ссылаясь на беседы с сотрудниками Национальной ассоциации уполномоченных по страхованию, в отчете GAO за май 2021 года отмечается отсутствие единообразия в том, как отрасль определяет ключевые термины политики, включая «акт войны». Эта двусмысленность может привести к недоразумениям и судебным разбирательствам между страховщиками и страхователями», — написало GAO, имея в виду судебные процессы, вызванные атакой NotPetya.

В ноябре 2021 года лондонская перестраховочная компания Lloyds выступила за исключения из закона о войне. Перестраховочные фирмы страхуют своих клиентов из страховой индустрии в способности оплачивать претензии. Стремясь ограничить свою подверженность риску, страховые компании, следуя их примеру, продолжали использовать исключение, поскольку эпидемия программ-вымогателей поразила поставщиков критической инфраструктуры.

В других случаях отрасль также подвергалась критике со стороны некоторых наблюдателей за то, что, как сообщается, поощряла страхователей выплачивать требования о выкупе. Министерство финансов также было предупреждено, что страховые компании могут нарушать санкции США, взаимодействуя с запрещенными режимами, такими как Северная Корея и Иран, по доверенности, когда они осуществляют такие платежи.

Представители страховой отрасли говорят, что они проводят более тщательную проверку во время своих процедур андеррайтинга в ответ на рост числа программ-вымогателей, а наблюдатели, такие как агентство кредитного рейтинга Moody's, сообщают, что война в Украине, наряду с программами-вымогателями, привела к сужению охвата и повышению страховых взносов. из промышленности. Представители страховых компаний также отмечают поправки, внесенные Lloyds в свой бюллетень в августе, в которых рекомендуется использовать более четкие формулировки «акта войны» в страховых полисах.

«Мы признаем, что многие управляющие агенты на рынке уже включают в свои полисы положения, специально предназначенные для исключения подверженности кибератакам, возникающим как в результате военных, так и невоенных кибератак, поддерживаемых государством», — написал перестраховщик. «Однако мы хотим убедиться, что все синдикаты, пишущие в этом классе, делают это в соответствии с надлежащим стандартом, с надежными формулировками… сложности, которые могут возникнуть в результате разоблачения кибератак в контексте войны или не войны, атак, поддерживаемых государством. означает, что андеррайтеры должны обеспечить юридическую проверку своих формулировок, чтобы убедиться, что они достаточно надежны».

Поскольку январское решение суда, недавнее соглашение об урегулировании и атаки на цепочку поставок, такие как взлом SolarWinds, подчеркивают эффективность отрасли в управлении рисками кибербезопасности, страховые компании продвигают федеральный ответ, чтобы дополнить свое покрытие.

«Страховая отрасль прошла долгий путь в своем понимании кибертерроризма, [враждебной киберактивности] и кибервойны, а также в оценке того, как застраховать такие риски», — говорится в отчете Женевской ассоциации, аналитического центра страховой отрасли, опубликованном в январе. «Чтобы расширить пределы страховой возможности, страховщики должны активно оценивать возможные варианты распределения киберрисков, в том числе с правительствами через [государственно-частное партнерство]. Такие совместные усилия страховщиков и правительств позволят сократить пробелы в киберзащите и обеспечат полную реализацию социальных преимуществ киберпространства».

Ссылаясь на уведомление Министерства финансов и CISA, глобальная страховая компания Swiss Re выразила свою поддержку федеральной программе страхования в отчете от 8 ноября.

«Акты кибервойны, нарушение работы облачного поставщика критически важного программного обеспечения или развертывание вредоносного ПО через широко используемое программное обеспечение являются примерами сценариев, которые могут привести к катастрофическим потерям», — говорится в отчете, отмечая «потенциальное решение, которое поможет закрыть защиту». пробел заключается в разработке схемы страхования типа государственно-частного партнерства (ГЧП), в которой покрытие системных рисков делится между страховщиками и фондом, поддерживаемым государством».

Казначейство и CISA обращают внимание на призывы отрасли. Их запрос на комментарий от 29 сентября ссылается на отчет Женевской ассоциации, в котором говорится, что успешная федеральная программа киберстрахования должна также побуждать организации приобретать киберстрахование.

«Чтобы стимулировать хорошую кибербезопасность, как можно больший риск должен оставаться за фирмами и отдельными лицами и должен быть гарантирован частными страховщиками на коммерческих условиях, а участие государственного сектора ограничено экстремальными потерями», — говорится в отчете группы. «Любые решения, поддерживаемые государством, должны быть не просто фискальными, но и вместе со страховщиками способствовать внедрению передового опыта в области кибербезопасности, включая получение надлежащего страхования, чтобы снизить уязвимость общества к таким рискам».

В запросе Министерства финансов и CISA о комментариях также спрашивается, как федеральная программа страхования может избежать создания морального риска, который они описывают как «возможность того, что страховщики или держатели полисов могут пойти на неоправданный риск, полагаясь на ответ федерального страхования, или не внедрить средства контроля кибербезопасности.»

Рекомендуя агентствам отчитываться перед Конгрессом о достоинствах федеральной страховой программы, GAO посоветовало проявлять осторожность в отношении проблемы морального риска». ***(Mariam Baksh. Agencies Push Deadline to Comment on Would-Be Federal Cyber Insurance Program // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/agencies-push-deadline-comment-would-be-federal-cyber-insurance-program/379858/). 18.11.2022).***

***

Кіберзахист критичної інфраструктури

«Агентство также предложило консолидировать существующие секторы и указало на необходимость наделения некоторых агентств большей властью над организациями частного сектора.

Ведущим должностным лицам в области кибербезопасности и управления отраслевыми рисками следует рассмотреть возможность создания космоса и биоэкономики в качестве двух новых секторов критической инфраструктуры,

говорится в отчете Агентства по кибербезопасности и безопасности инфраструктуры для президента Джо Байдена и соответствующих комитетов Конгресса.

«Результаты подчеркивают возможность выделения космического сектора и сектора биоэкономики в зависимости от описанного процесса проверки», — пишет CISA, рекомендуя критерии, такие как возможность сбоев в различных секторах экономики США, которые могут оказать пагубное воздействие на общество, — при принятии решений. определения критической инфраструктуры.

Что касается той части экономики, которая зависит от биологических ресурсов, таких как растения и микроорганизмы, обеспечение безопасности биоэкономики будет включать усилия по решению таких проблем, как изменение климата и производство продуктов питания.

Организации в секторах, определенных как критическая инфраструктура, и назначенные им агентства по управлению отраслевыми рисками, или SMA, могут получить больше ресурсов и нести большую регулирующую ответственность в соответствии с предлагаемой эволюцией федеральной политики кибербезопасности.

«Несколько секторов предлагают фрагментированное или частичное представление о более широком масштабе, связанном с общими функциями, и поэтому может быть выгодно рассмотреть возможность слияния или консолидации этих секторов», — также подчеркнула CISA, отметив в качестве одного из примеров сектор аварийно-спасательных служб, поскольку он «содержит услуги, в основном предоставляемые или контролируемые государственными органами».

На отчет, полученный Nextgov, ссылались в письме президента Байдена от 7 ноября, адресованном Конгрессу, в котором отмечалось его намерение выполнить его рекомендации. Секретарь Министерства внутренней безопасности должен был представить отчет в соответствии с Законом о государственной обороне 2021 года. Положение NDAA подтолкнуло постоянное обязательство DHS в соответствии с Законом о внутренней безопасности и директивой президента 2013 года — PPD 21 — разработать и обновить национальный план по обеспечению безопасности ключевых ресурсов и защите критически важной инфраструктуры.

В сентябре 2021 года генеральный инспектор DHS вызвал CISA за то, что он не обновлял план более восьми лет. Отвечая генеральному инспектору, директор CISA Джен Истерли заявила, что план будет готов к 30 сентября 2022 года. В предыдущем отчете CISA предполагала, что план будет готов к декабрю 2020 года, сообщил генеральный инспектор.

Секретарь DHS имеет право назначать новые сектора критической инфраструктуры, как это сделал бывший секретарь DHS Джех Джонсон в 2017 году, назвав выборы подсектором сектора государственных услуг. Но CISA, как указано в отчете, требуемом NDAA, хочет, чтобы такие обязанности по координации защиты критической инфраструктуры были разделены между Управлением национального кибер-директора — также просроченным для разработки национальной стратегии — Советом национальной безопасности и агентствами, которые делают Федеральный совет высшего руководства.

«CISA, в сотрудничестве с ONCD, NSC и SMA, а также при участии других соответствующих департаментов и агентств, должна… оценить объем текущих секторов критической инфраструктуры, чтобы убедиться, что они надлежащим

образом учитывают системы, активы, национальные критические функции и возможности; оценить потенциальные модификации обозначений SRMA; и оценить потенциальное создание новых секторов или подсекторов», — пишет CISA.

CISA возложила ответственность за управление отраслевыми рисками более чем на половину текущего набора из 16 важнейших секторов инфраструктуры, некоторые из которых, например, секторы связи и информационных технологий, не имеют регулирующих полномочий.

Некоторые законодатели, в первую очередь член палаты представителей Ричи Торрес, DN.Y., поставили под сомнение способность CISA взять на себя такую большую ответственность за обеспечение безопасности критически важной инфраструктуры в отсутствие дополнительных полномочий.

Другие в Конгрессе обсудили необходимость пересмотра PPD 21, чтобы лучше управлять рисками в информационных и коммуникационных технологиях. А заместитель советника по национальной безопасности по кибербезопасности и новым технологиям Энн Нойбергер и национальный директор по кибербезопасности Крис Инглис предположили, что таким организациям неминуемо более широкое применение регулирующих полномочий.

В отчете CISA президенту и комитетам рассматриваются эти вопросы, при этом отмечается, что последовательное использование его критериев для назначения агентств по защите критически важной инфраструктуры должно опираться «на все необходимые возможности и полномочия федеральных департаментов и агентств». Он также должен обеспечить, чтобы национальный план «не слишком полагался на полномочия одного департамента или агентства по управлению участием сектора».

«Закон о национальной безопасности, PPD-21 и национальный план признают, что регулирующие полномочия и возможности являются основными причинами, по которым федеральное агентство будет назначено SRMA в данном секторе», — добавила CISA. «Точно так же SRMA и DHS несут ответственность за определение соответствующих мер противодействия инфраструктурным угрозам и уязвимостям».

В сентябре CISA опубликовала план деятельности агентства на следующие три года. В этом плане особое внимание уделялось измерению эффективности целевых показателей производительности, установленных CISA для критической инфраструктуры, владеющей промышленными системами управления, уязвимыми для разрушительных атак. Но агентство не сообщило, как оно намеревается выполнить свои цели измерения, и в его отчете президенту говорится, что в текущем плане оценки безопасности критически важной инфраструктуры в рамках SRMA есть ограничения.

В отчете CISA также подчеркивается наличие у нее различных базовых возможностей и услуг, в том числе для «выявления и снижения рисков кибербезопасности, таких как сканирование уязвимостей, тестирование на проникновение и анализ архитектуры.

В отчете особо рекомендуется провести оценку необходимости в дополнительных полномочиях в соответствии с предложением Комиссии Cyberspace Solarium по выявлению «системно важных объектов» критической инфраструктуры для регулирования.

Такие органы могут уполномочить секретаря DHS «в консультации с руководителями соответствующих SRMA по мере необходимости… назначать высокоприоритетную инфраструктуру, направлять федеральные ресурсы на назначенную инфраструктуру и требовать определенных действий от владельцев и операторов таких [SIE]».

Секретарь министерства внутренней безопасности Алехандро Майоркас, получив возможность обсудить, как Конгресс мог бы надлежащим образом усилить федеральные полномочия во время слушаний во вторник, возразил». ***(Mariam Baksh. CISA Highlights Space, Bioeconomy as Possible New Critical Infrastructure Sectors // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/cisa-highlights-space-bioeconomy-possible-new-critical-infrastructure-sectors/379818/). 16.11.2022).***

***

«Официальные лица CISA и DARPA рассказали о своих инициативах по поддержке операций кибербезопасности в сетях критической инфраструктуры.

На состоявшемся в среду заседании Совета советников президента по науке и технологиям были заслушаны мнения экспертов о лучшем построении киберустойчивой цифровой инфраструктуры на национальном уровне, при этом нынешние правительственные чиновники выступали за сочетание новых технологий и снижения рисков.

Агентство перспективных оборонных исследовательских проектов возглавило усилия по укреплению критической инфраструктуры с помощью передовой аналитики данных и технологий кибербезопасности.

Кэтлин Фишер, директор отдела информационных инноваций DARPA, описала эксперимент, в ходе которого ее офис разработал сенсорные инструменты, предназначенные для электросетей, чтобы отличать кибератаки от погодных инцидентов.

«Сбои, вызванные природой и несчастными случаями, действительно сильно отличаются от сбоев, вызванных киберпреступником, потому что киберпреступник может заставить систему лгать», — сказала она во время своей презентации.

DARPA протестировало новый датчик и соответствующий алгоритм для моделирования энергосистем в своей программе Rapid Attack Detection, Isolation and Characterization Systems или RADICS. RADICS удалось обучить энергетиков запускать скомпрометированную электросеть или возвращать часть электросети в работу без использования внешней энергии из-за кибератаки.

Технология RADICS была разработана для обнаружения неверных данных, изоляции скомпрометированных каналов связи и узлов, а также внедрения новых методов анализа трафика и ИТ-протоколов. Фишер сказал, что алгоритм DARPA RADICS в настоящее время используется несколькими коммунальными компаниями и независимыми государственными системными операторами.

Ключевая функция предоставила операторам электросетей средства для проведения криминалистического анализа с помощью как программного, так и аппаратного обеспечения для оценки кибератак на систему и помощи в восстановлении работы сети в короткие сроки.

«RADICS был хорошим началом, но в этой области еще предстоит проделать большую работу, в том числе продолжить разработку возможностей быстрого моделирования на основе внеполосных датчиков, чтобы обеспечить надежную ситуационную осведомленность, возможности глубокого криминалистического анализа и продолжение партнерства между энергетиками. и кибер-эксперты, с возможностью практиковаться и выполнять боевые упражнения», — сказала она.

Коллеги-эксперты повторили необходимость улучшения цифровой защиты критической инфраструктуры, в основном за счет более целостного подхода, ориентированного на организацию.

Дэвид Массингтон, исполнительный помощник директора по безопасности инфраструктуры в Агентстве кибербезопасности и безопасности инфраструктуры, отметил, что в последние несколько лет наблюдается все более серьезные кибератаки на критически важную инфраструктуру и учреждения США. CISA отреагировала на эти растущие угрозы с помощью отраслевых мер по смягчению последствий, чтобы сосредоточиться на уникальных проблемах, с которыми сталкивается каждая отрасль.

«Мы беспокоимся о рисках, системах, которые предоставляют жизненно важные цифровые и другие услуги, такие как американская экономика, в частности», — сказал он. «Мы беспокоимся об этом, потому что это сложная среда риска, которая позволяет конкретным злоумышленникам, из национальных государств и других, прерывать доступность критически важных данных и услуг».

Массингтон подчеркнул деятельность CISA по управлению отраслевыми рисками как попытку изучить снижение рисков критической инфраструктуры в различных секторах. Примеры включают Министерство внутренней безопасности, контролирующее критически важные производственные системы, и Министерство транспорта, контролирующее транспортную инфраструктуру.

Целью этих мер устойчивости является разработка планов по поддержанию товарного потока из секторов. Перед CISA и Министерством внутренней безопасности поставлена задача содействовать этим критическим оценкам инфраструктуры, чтобы определить, насколько они подвержены риску.

«Большая часть национальной координационной деятельности, которую осуществляет CISA, направлена на выявление уязвимых мест и рисков, а также на координацию сотрудничества для снижения приоритетных рисков», — продолжил он. «Обмен передовым опытом в отрасли — это действительно наша работа».

Джим Платт, исполняющий обязанности заместителя директора Национального центра управления рисками CISA, добавил, что подход к управлению рисками с точки зрения результатов, то есть определение того, что конкретно производит каждый отдельный сектор инфраструктуры, может лучше укрепить их системные возможности.

«Нам нужно взглянуть на это с функциональной точки зрения, — сказал Платт. «Что обеспечивают эти критически важные инфраструктурные сектора? И [мы] смотрим на них с точки зрения всех опасностей и обеспечиваем непрерывность операционных процедур по мере продвижения вперед». ***(Alexandra Kelley. How Federal Agencies are Using Innovative Tech to Protect Critical Infrastructure Cybersecurity // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/how-federal-***

agencies-are-using-innovative-tech-protect-critical-infrastructure-cybersecurity/379588/). 10.11.2022).

***

«Существует только один верный способ снизить риски, связанные с оборудованием, — комплексное тестирование на проникновение.

Недавно Вергл Гипсон, старший советник центра интеграции Cybercore в Национальной лаборатории Айдахо, дал показания перед подкомитетом внутренней безопасности Палаты представителей по кибербезопасности, защите инфраструктуры и инновациям. Он пришел к выводу, что системы операционных технологий в США более уязвимы для вредоносных кибератак, чем информационные технологии. Это заявление вызывает особую тревогу, поскольку большая часть критически важной инфраструктуры в мире стала целью кибератак.

В глобальном масштабе было предпринято множество попыток кибератак на глобальные сети и коммунальные услуги, многие из которых были связаны с фишингом и программами-вымогателями, и некоторые из них были успешными. В отчете о глобальных рисках Всемирного экономического форума кибератаки на критическую инфраструктуру (КИ) названы главной проблемой. ВЭФ отметил, что «атаки на критически важную инфраструктуру стали новой нормой в таких секторах, как энергетика, здравоохранение и транспорт». Отчет о глобальных рисках 2020 Всемирный экономический форум (weforum.org)

Угроза критической инфраструктуре и особенно энергетике

Энергетический сектор выделяется как наиболее уязвимый среди важнейших инфраструктур. Эта энергетическая экосистема включает электростанции, коммунальные предприятия, атомные электростанции и сеть. Защита критически важных промышленных систем управления (ICS), операционных технологий (OT) и ИТ-систем от угроз кибербезопасности — непростая задача. Все они имеют уникальные операционные структуры, точки доступа и множество устаревших систем и новых технологий.

В отчете Ponemon сообщается, что три четверти энергетических компаний и коммунальных служб сталкивались как минимум с одной недавней утечкой данных. Одним из факторов является растущая изощренность злоумышленников. Одна из причин, по которой энергетический сектор стал более уязвимым, заключается в том, что хакеры получили более глубокие знания о системах управления и конвергентных архитектурах OT и ИТ, а также о том, как они могут быть атакованы и могут использовать вооруженные вредоносные программы против электростанций и других объектов, связанных с энергетикой. ресурсы.

Агентство национальной безопасности (АНБ) недавно выпустило рекомендации по кибербезопасности именно по этому вопросу интеграции и подключения OT и ИТ-систем. В рекомендациях подробно рассказывается, «как оценивать риски для систем и повышать безопасность соединений между OT и корпоративными сетями. Эксплуатация информационных технологий (ИТ) может служить отправной точкой для эксплуатации OT, поэтому для обеспечения соблюдения уникальных требований кибербезопасности необходима тщательная оценка риска подключения между ИТ- и OT-системами».

«Каждое подключение IT-OT увеличивает потенциальную поверхность атаки. Чтобы предотвратить опасные результаты использования OT, операторы OT и системные администраторы ИТ должны гарантировать, что разрешены только самые обязательные подключения IT-OT, и что они максимально защищены. Примером такого типа угроз является недавнее использование со стороны злоумышленников программного обеспечения для управления ИТ и его цепочки поставок в результате компрометации SolarWinds с публично задокументированными последствиями для OT, включая критически важную инфраструктуру США».

«АНБ рекомендует предпринимать шаги по улучшению кибербезопасности для сетей OT, когда подключение IT-OT имеет решающее значение в соответствии с их уникальными потребностями. Для подключений IT-OT, которые считаются необходимыми, следует предпринять шаги для снижения рисков путей эксплуатации IT-OT. Смягчающие меры включают полное управление всеми подключениями IT-OT, ограничение доступа, активный мониторинг и регистрацию всех попыток доступа, а также криптографическую защиту векторов удаленного доступа». АНБ выпускает рекомендации по кибербезопасности по обеспечению безопасности операционных технологий > Центральная служба безопасности Агентства национальной безопасности > Просмотр статьи

Существует только один верный способ снизить риски, связанные с оборудованием, — комплексное тестирование на проникновение. Тестирование выявляет уязвимости и позволяет понять киберриски в среде критической инфраструктуры.

Показательный пример: проверка аппаратной кибербезопасности на KVM-устройствах, подключенных к критически важной инфраструктуре.

Чтобы обеспечить безопасность в условиях растущего ландшафта угроз, аппаратная киберзащита необходима в критической инфраструктуре OT. Лучший способ узнать, безопасна ли OT, — это сделать это с помощью тестирования на проникновение. Недавно Израильская электрическая корпорация (IEC) инициировала тестирование своих потенциальных поставщиков на проникновение, чтобы проверить, насколько хорошо они защищены от взломов.

Как крупнейший поставщик электроэнергии в Израиле, который строит, обслуживает и эксплуатирует электростанции, подстанции, а также передающие и распределительные сети, IEC не может позволить себе развертывание технологий безопасности, которые не соответствуют спецификациям миссий. Это особенно важно, поскольку критическая инфраструктура Израиля ежедневно подвергается изощренным атакам, а уязвимости аппаратных продуктов, которые теперь связаны с критической инфраструктурой, могут представлять серьезную угрозу, если их обнаружат и воспользуются злоумышленниками.

IEC провела тесты на проникновение защищенных KVM, которые они приобрели у одного из двух единственных в Израиле производителей защищенных KVM, чьи продукты используются на американском рынке безопасности. К их удивлению, поставщик, заявивший, что его защищенные KVM непробиваемы, не прошел тест, определяющий, является ли KVM однонаправленным или двунаправленным. KVM не прошли тест с использованием скомпрометированного кабеля и не смогли остановить попытку взлома драйверов KVM. Главный результат

заключается в том, что хакеры могут легко обойти драйверы операционной системы и взломать сети OT. Поставщику был предоставлен второй шанс оценить свое KVM-устройство после того, как оно вышло из строя, но оно по-прежнему не соответствовало требованиям безопасности.

По запросу IEC компания Fibernet, другой израильский производитель защищенных KVM, предложила устройства для тестирования и прошла проверку, поскольку на самом деле у них была аппаратная кибербезопасность, необходимая для защиты систем OT и SCADA.

Fibernet, израильский разработчик и производитель волоконной оптики, безопасных AV и решений для центров обработки данных, хорошо известен как в центрах обработки данных, так и в сфере кибербезопасности, а среди известных клиентов компании — престижная Европейская лаборатория физики частиц — CERN, IDF, и правительство Израиля.

Должная осмотрительность в области физической безопасности является необходимым шагом к настройке и защите критической инфраструктуры и особенно к тому, какие аппаратные устройства подключены к сетям. Неавторизованное или небрежно подключенное к сети устройство обеспечивает простой способ экономического шпионажа и дает хакерам возможность для кражи данных.

Потенциальное введение поставщиком в заблуждение для Israel Electric Company является тревожным звонком для каждого глобального оператора, участвующего в обеспечении безопасности OT SCADA, который полагается на своих поставщиков в отношении правдивых заявлений о возможностях и характеристиках производительности их решений кибербезопасности. Для критической инфраструктуры и операций OT и SCADA это предостережение о кибербезопасности или осторожность покупателя, которое требует тщательного тестирования на проникновение и проверки среди всех поставщиков, прежде чем устройства будут закуплены». ***(Chuk Brookx. COLUMN: Test and Verify That Cybersecurity Products Can Protect Critical Infrastructure // Homeland Security Today (https://www.hstoday.us/featured/column-test-and-verify-that-cybersecurity-products-can-protect-critical-infrastructure/). 07.11.2022).***

***

«Ошибки в написании нескольких доменов портовых сооружений США «недавно были зарегистрированы, вероятно, в злонамеренных целях», сообщило киберкомандование Береговой охраны США.

На прошлой неделе отдел разведки киберкомандования береговой охраны предупредил морские заинтересованные стороны о том, что кампании по типосквоттингу, проводимые киберпреступниками, по-прежнему нацелены на морскую транспортную систему.

Typosquatting предназначен для людей, которые, как следует из названия, делают ошибку при вводе URL-адреса в веб-браузере. Затем пользователи могут быть перенаправлены на вредоносный веб-сайт, который включает в свой URL-адрес распространенную опечатку, но при этом выдает себя за законный веб-сайт. Оказавшись на поддельном веб-сайте, пользователь может быть обманут и раскрыт конфиденциальной информации.

В информационном бюллетене Maritime Cyber Alert 01-22, выпущенном киберкомандованием береговой охраны США в марте, сообщается о «недавнем всплеске числа злоумышленников, использующих поддельные бизнес-сайты для атаки на морскую транспортную систему (MTS)».

«Несколько партнеров МТС обнаружили хорошо сконструированные поддельные веб-сайты, маскирующиеся под их законные деловые веб-сайты. Эти сайты создаются предположительно для кражи информации или установки вредоносных программ на устройства клиентов, взаимодействующих с сайтами», — говорится в предупреждении. «Эти поддельные веб-сайты не предназначены для прямого воздействия на морскую организацию, но напоминают атаки в стиле водопоя, когда предполагаемыми целями являются физические и юридические лица, посещающие сайт. Поддельные веб-сайты выглядят профессионально и довольно сложно, некоторые из них представляют собой домены.com. Такой уровень детализации может затруднить отличить настоящий сайт от мошеннического».

В прошлую пятницу USCG заявила, что атаки продолжаются, поскольку «злоумышленники продолжают подделывать домены портовых сооружений США, используя методы опечатки, пытаясь перенаправить пользователей на вредоносные веб-сайты с похожими доменными именами».

Ошибки в написании нескольких доменов портовых сооружений США «недавно были зарегистрированы, вероятно, в злонамеренных целях», сообщил разведывательный отдел киберкомандования USCG, и «эти события были проанализированы и расследованы».

Одним из способов предотвращения опечаток является то, что морская организация заявляет о распространенных опечатках до того, как это сделают злоумышленники.

«Организации могут намеренно регистрировать домены, похожие на их собственные, чтобы удержать злоумышленников от создания доменов с опечатками», — говорится в заявлении Береговой охраны США. «Другие аспекты этого метода нельзя легко смягчить с помощью превентивных средств контроля, поскольку он основан на поведении, выполняемом вне сферы защиты и контроля предприятия».

Береговая охрана США также рекомендовала морским организациям рассмотреть возможность использования таких сервисов, как базы данных WHOIS, которые могут помочь отслеживать недавно приобретенные домены. «В некоторых случаях можно использовать известные части информации о регистрации домена, чтобы раскрыть другую инфраструктуру, купленную злоумышленником», — отмечается в предупреждении. «Рассмотрите возможность мониторинга доменов, созданных со структурой, аналогичной вашей, в том числе в другом TLD».

USCG также рекомендовала морским предприятиям помнить о кибергигиене, в том числе избегать переходов по ссылкам от третьих лиц. «Рассматривайте весь трафик, проходящий через вашу сеть, особенно сторонний трафик, как ненадежный до тех пор, пока он не будет подтвержден как законный», — говорится в заявлении Береговой охраны США.

О кибер-событиях можно сообщать местному капитану береговой охраны порта или круглосуточному дежурному киберкомандованию береговой охраны по телефону 202-372-2904 или по электронной почте CyberWatch@uscg.mil.

«Ваша готовность соблюдать требования и своевременно отчитываться помогает США реагировать быстро и эффективно и делает критически важную морскую инфраструктуру более безопасной», — заявили в USCG». ***(Bridget Johnson. Coast Guard Warns of Malicious Typosquatting Directed at Port Facility Websites // Homeland Security Today (https://www.hstoday.us/featured/coast-guard-warns-of-malicious-typosquatting-directed-at-port-facility-websites/). 11.11.2022).***

***

Кіберзахист закладів охорони здоров'я

«Международный комитет призывает преступников рассматривать символ Красного Креста как запретное

Всемирно признанный символ Красного Креста помечал людей и объекты, недоступные для нападения на протяжении столетия войн, но эксперты по безопасности скептически относятся к недавнему предложению создать цифровой маркер Красного Креста для защиты медицинских и гуманитарных организаций от кибератак. Причина? Нельзя доверять киберпреступникам.

В отчете, опубликованном в четверг, Международный комитет Красного Креста предложил применять цифровой маркер Красного Креста к веб-сайтам, системам и конечным точкам, используемым в медицинских и гуманитарных целях.

«Эмблемы красного креста и красного полумесяца — простой красный крест или красный полумесяц, нарисованные на крыше больницы или автомобиля, — долгое время служили знаком защиты, — говорит Роберт Мардини, генеральный директор МККК. — Я испытал на себе эту защитную силу. эмблемы из первых рук во многих деликатных ситуациях: например, когда мы способствовали эвакуации гражданских лиц из осажденного сельского Дамаска, Сирия, в 2018 году, когда мы вошли в осажденный город Таиз, Йемен, в 2017 году, или в ходе моего много визитов в сектор Газа».

Рекомендация Красного Креста последовала за растущими атаками программ-вымогателей на медицинские учреждения, а также усилением роли кибервойны после российского вторжения в Украину. В предложении содержится призыв к тому, чтобы злоумышленники могли легко найти этот символ, не будучи обнаруженными группами кибербезопасности, а также упростить его развертывание для учреждений здравоохранения и оказания помощи.

Проблема в том, что проект потребует сотрудничества огромного количества злоумышленников, атакующих здравоохранение. Хотя национальные государства взаимно признают символ Красного Креста на поле боя, между жертвами и преступниками не существует таких отношений, говорит Майкл Гамильтон, директор по информационной безопасности Critical Insight.

«Их намерение состоит в том, чтобы создать аналогию с символом, используемым на полях сражений, но, на мой взгляд, это мало что даст в качестве

сдерживающего фактора», — говорит Гамильтон. «Больницы особенно преследуются из-за их критичности и, следовательно, готовности платить за вымогательство».

Красный Крест заявляет, что цифровая эмблема должна обозначать различные цифровые компоненты, такие как серверы, компьютеры, смартфоны, устройства IoT и сетевые устройства, а также цифровые услуги, такие как FTP-серверы и VPN, облачную инфраструктуру и коммуникационное оборудование.

Кроме того, система должна быть настроена таким образом, чтобы злоумышленники могли исследовать цифровую эмблему, не идентифицируясь как субъекты угрозы. «Другими словами, если кибероператоры обеспокоены тем, что поиск цифровой эмблемы позволит их идентифицировать, они не будут ее искать», — говорится в отчете.

К сожалению, по словам Эррола Вайса, начальника службы безопасности Healthcare-ISAC, большинство злоумышленников используют метод дробовика с электронными письмами, которые могут достигать миллионов людей, и как только кто-либо становится жертвой фишинговой атаки, их приоритетом является усиление позиций и поиск путей. монетизировать нарушение.

«Возможно, как только они поймут, к чему они получили доступ, возможно, они прекратят атаку, но я так не думаю», — говорит Вайс, добавляя, что киберпреступники публично объявили перемирие в отношении здравоохранения в разгар пандемии COVID-19. «Конечно, мы видели, что все это длилось около нуля минут. Они нападали на больницы, и мы видели, как больницы брали выкуп, поэтому я не вижу, чтобы они вообще соответствовали этому».

В отчете Красного Креста рассматриваются три способа развертывания маркеров: эмблема на основе DNS, связанная с доменным именем, эмблема на основе IP-адреса, которая потребует встраивания семантики в IP-адреса для идентификации как защищенных цифровых активов, так и защищенных сообщений, или аутентифицированный цифровая эмблема, основанная на распределенном подходе, использующем цепочки сертификатов и самозаверяющие эмблемы, которые ссылаются на открытые ключи.

Эмблема не должна заменять инвестиции в системы и методы кибербезопасности. «Поскольку безопасность ИКТ требует инвестиций и опыта, существует риск того, что некоторые организации могут предпочесть полностью полагаться на цифровую эмблему вместо принятия других основных мер безопасности», — говорится в отчете. «Таким образом, цифровая эмблема может создать ложное ощущение защиты или безопасности».

Гамильтон из Critical Insight говорит, что безопасность должна быть главным приоритетом. «Отрасль знает, что ей нужно сделать, чтобы защитить себя, но не может сделать это в одиночку, когда доходы и прибыль пострадали так сильно», — говорит он. «Федеральное правительство должно продолжать усилия по санкционированию криптовалютных бирж, используемых для платежей программ-вымогателей, защищать дальнейшие действия, используя ресурсы Министерства обороны, задерживать и преследовать в судебном порядке вместе с Министерством юстиции, а также использовать риторические конструкции, такие как призыв к

использованию программ-вымогателей против критической инфраструктуры, а не терроризм. чем преступление, и относитесь к нему как к таковому».

Киберпреступники продемонстрировали свою готовность избегать атак на здравоохранение, которые могут угрожать жизни, таких как атака программы-вымогателя на Ирландскую службу здравоохранения в 2021 году, когда преступники предоставили группе больниц дешифратор для восстановления зараженных систем. Но Падраик О'Рейли, соучредитель CyberSaint Security, указывает, что преступники также планировали нападение на детскую больницу Бостона.

«Я не очень верю в щепетильность банд вымогателей, — говорит О'Рейли. «Чем ценнее данные для пострадавшей организации и пациентов, которых она обслуживает, тем вероятнее день выплаты жалованья. В 2021 году более половины пострадавших организаций здравоохранения заплатили выкуп, но многие не получили свои полные данные. волшебная палочка здесь за пределами действительно укрепляющих систем и в первую очередь обеспечения того, чтобы банды не получили доступ к системам». ***(Cal Harrison. Could a Digital Red Cross Protect Hospitals From Ransomware? // Information Security Media Group, Corp. (https://www.govinfosecurity.com/could-digital-red-cross-protect-hospitals-from-ransomware-a-20442). 09.11.2022).***

***

«Группа, утверждающая, что связана с REvil, угрожает раскрыть данные

Крупнейшая в Австралии частная медицинская страховая компания заявляет, что не будет платить за вымогательство со стороны хакеров, угрожающих раскрыть личные данные миллионов нынешних и бывших клиентов.

Medibank опубликовал заявление, в котором поясняется, что, по его мнению, выплата может «побудить преступника напрямую вымогать деньги у наших клиентов, и существует большая вероятность того, что выплата нанесет вред большему количеству людей, сделав Австралию более крупной мишенью».

Шансы на выплату в результате возврата данных о клиентах, которые, по словам Medibank, в настоящее время охватывают 9,7 миллиона человек, «ограничены», заявляет компания.

Сайт утечки вымогателей в даркнете пообещал начать утечку украденных данных в течение 24 часов.

Общее число пострадавших составляет 5,1 миллиона клиентов Medibank, около 2,8 миллиона клиентов ahm и около 1,8 миллиона международных клиентов, которым требуется частное медицинское страхование во время проживания или учебы в Австралии.

В этих итогах содержатся данные о заявлениях о здоровье для 160 000 клиентов Medibank, около 300 000 клиентов и около 20 000 международных клиентов. Эти данные включают коды, связанные с диагнозами и процедурами.

По словам Medibank, в набор данных не включены данные платежной или банковской карты или первичные документы, удостоверяющие личность.

По крайней мере, по названию сайт утечки темной паутины связан с REvil — также известной как Sodinokibi — печально известной бандой программ-

вымогателей, разгромленной западными правоохранительными органами в июле 2021 года (см. Расформирован ли REvil? Белый дом говорит, что не знает).

В апреле этого года кто-то перезапустил сайты Tor REvil. Исследователи по борьбе с программами-вымогателями из команды Malware Hunter Team сообщают, что несколько операций теперь используют утечку кода REvil, что затрудняет атрибуцию любой атаки, в которой он используется.

Страховщик не раскрыл сумму требования о вымогательстве, а генеральный директор Дэвид Кочкар обратился к национальному телевидению, чтобы назвать цифру в долларах неважной.

«Сумма денег, которую требовали, на самом деле не имела отношения к решению. Решение было основано на совете эксперта по киберпреступности», — сказал он.

Поддержала Medibank министр внутренних дел Клэр О'Нил, которая в Твиттере назвала это решение «согласующимся с рекомендацией правительства Австралии».

«Я хочу, чтобы Австралия была самой кибербезопасной страной в мире. Выплата выкупа напрямую подрывает эту цель».

Международная конференция по борьбе с программами-вымогателями, состоявшаяся в Белом доме США, завершилась в прошлый вторник тем, что Австралия пообещала возглавить целевую группу по обмену ранними предупреждающими признаками атак программ-вымогателей.

Похоже, что Австралия переживает волну киберинцидентов, хотя есть данные, свидетельствующие о том, что страна ощущает последствия серии оппортунистических атак, а не скоординированной атаки.

Австралийский центр кибербезопасности в ежегодном правительственном отчете, опубликованном в пятницу, сообщил, что во второй половине 2021 и первой половине 2022 года количество сообщений о киберпреступлениях увеличилось на 13% по сравнению с тем же периодом годом ранее. Общее количество составило более 76 000 сообщений о киберпреступлениях.

Об этом сообщает Мэтью Шварц из ISMG». ***(Mihir Bagwe. Medibank Says No to Paying Hacker's Extortion Demand // Information Security Media Group, Corp. (https://www.govinfosecurity.com/medibank-says-no-to-paying-hackers-extortion-demand-a-20424). 07.11.2022).***

***

«Тегеранские хакеры используют социальную инженерию, чтобы закрыть пробел в уровне сложности

Федеральное правительство предупреждает сектор здравоохранения о том, что будьте начеку иранские субъекты угрозы, одетые как врачи, исследователи аналитических центров или репортеры.

Координационный центр кибербезопасности сектора здравоохранения Министерства здравоохранения и социальных служб на брифинге по угрозам в четверг заявил, что хакеры, поддерживаемые Тегераном, часто полагаются на социальную инженерию для проникновения в цели, в том числе в больницы.

Один из недавних инцидентов связан с кампанией группы угроз, получившей название Tortoiseshell, с участием учетных записей Facebook, выдающих себя за вербовщиков для медицины, журналистики и других отраслей. Американские и европейские мишени получали файлы, зараженные вредоносным ПО, или их заманивали ввести конфиденциальные учетные данные на фишинговых сайтах (см.: Facebook прерывает иранскую кампанию APT).

«Иранские субъекты, спонсируемые государством, часто вкладывают значительные средства в уровни социальной инженерии своих атак», — говорит Пол Прюдомм, бывший аналитик по угрозам Министерства обороны, который возглавляет консультативный отдел разведки угроз в Rapid7.

«Иранские субъекты могут иметь менее сложные технические возможности, чем их коллеги в других странах, но компенсируют это более сложными и потенциально более убедительными схемами социальной инженерии».

Прюдомм говорит, что иранские деятели иногда идут на все, чтобы сделать своих персонажей социальной инженерии более достоверными, например, создавая для них дополнительные учетные записи в социальных сетях или другие элементы интернет-отпечатка помимо того, который использовался в атаке, в надежде выдержать проверку. «Распространенной формой иранской социальной инженерии является использование поддельной учетной записи LinkedIn для целей социальной инженерии с приманкой возможностей трудоустройства в соответствующих областях», - говорит он.

В одном примере, приведенном HC3, иранский хакер выдавал себя за директора по исследованиям Института исследований внешней политики. Доверие к фишинговому письму придало решение злоумышленника скопировать адрес электронной почты другого директора исследовательского центра Pew Research Center, который фактически привел к злоумышленнику.

Акцент на социальную инженерию не исключает проведения прямых атак. Одним из печально известных примеров была предотвращенная атака на Бостонскую детскую больницу в прошлом году — предотвращенная только потому, что власти США получили разведданные о готовящемся нападении и предупредили больницу, как заявил в июне директор ФБР Кристофер Рэй.

Хакеры использовали устройство Fortigate для доступа к больничным сетям контроля окружающей среды. Они получили доступ к известным учетным записям пользователей в больнице с IP-адреса, который ФБР связывает с иранским правительством.

Адам Мейерс, старший вице-президент по разведке в компании CrowdStrike, занимающейся безопасностью, сообщил Information Security Media Group, что атаки иранских злоумышленников, нацеленные на организации сектора здравоохранения, как правило, являются «более разрушительными операциями», чем атаки некоторых других хакеров, поддерживаемых государством, таких как Китай.

По его словам, часто атаки, связанные с Ираном, связаны с «блокировкой и утечкой», когда злоумышленники запускают программы-вымогатели, а затем сливают данные в первую очередь для дискредитации организации. По его словам, эти атаки иногда поддерживаются правительством Ирана или проводятся иранскими киберпреступными группировками. Атаки национального государства на сектор

здравоохранения часто были менее разрушительными, сосредоточившись на краже интеллектуальной собственности в отношении медицинских устройств, фармацевтических препаратов и других инноваций.

Эррол Вайс, начальник службы безопасности Центра обмена и анализа медицинской информации, говорит, что Иран обладает наступательными кибер-возможностями, а злоумышленники демонстрируют эффективные DDoS-атаки, разрушительные вайперы и другие кибератаки.

«Это группа субъектов угроз, на которую Health-ISAC обращает внимание, и мы работаем с несколькими партнерами, чтобы быть в курсе угроз, мотивов и методов атак, чтобы мы были лучше подготовлены и более устойчивы как сектор в случае, если здравоохранение станет мишенью».

В сентябре правительство США наложило санкции на министерство разведки и безопасности Ирана и его министра за июльскую кибератаку, которая временно парализовала портал онлайн-услуг Албании для граждан (см. Санкции США против иранских шпионов за кибератаку в Албании).

Мейерс говорит, что он подозревает, что рекомендации HHS HC3 направлены на то, чтобы привлечь внимание сектора здравоохранения к иранским угрозам, отчасти из-за этого нападения на Албанию». ***(Marianne Kolbasuk McGee. Feds Warn of Iranian Threats to Healthcare Sector // Information Security Media Group, Corp. (https://www.govinfosecurity.com/feds-warn-iranian-threats-to-healthcare-sector-a-20437). 08.11.2022).***

***

«Натиск фишинга вызвал нарушение, затронувшее 166 000 человек по всей стране

Поставщик медицинских услуг на дому и хосписов из Джорджии заплатит почти 500 000 долларов штату Массачусетс за прекращение судебного разбирательства в штате, связанного с утечкой данных, затрагивающей почти 170 000 пациентов.

Урегулирование произошло всего через несколько недель после того, как Aveanna Healthcare урегулировала в федеральном окружном суде предполагаемый коллективный иск на сумму до 800 000 долларов США в виде денежных выплат и защиты кредитного контроля.

Оба судебных дела связаны с потоком из 600 попыток фишинга, предпринятых летом 2019 года, которые со временем становились все более изощренными. В какой-то момент сотрудники компании получили электронное письмо, якобы от президента компании, с просьбой принять участие в опросе. В жалобе генерального прокурора Массачусетса говорится, что более 50 сотрудников стали жертвами двухмесячной атаки фишинга.

В предполагаемом групповом иске говорится, что фишерам сошли с рук данные пациентов, включая номера социального страхования, платежные реквизиты, идентификационные номера из паспортов и водительских прав, информацию о диагнозах и типе лечения.

В феврале 2020 года Aveanna сообщила в Министерство здравоохранения и социальных служб об инциденте, который затронул 166 077 человек, пациентов и сотрудников.

Каждое из поселений требует от Aveanna улучшения своей кибербезопасности. И Массачусетс, и предложенная групповая жалоба обвиняют компанию в том, что она не внедрила базовые средства защиты от кибербезопасности, включая многофакторную аутентификацию.

«Компании обязаны внедрить надлежащие меры и системы безопасности, чтобы предотвратить доступ хакеров к конфиденциальной информации», — заявила генеральный прокурор штата Массачусетс Маура Хили о соглашении своего офиса с Aveanna на сумму 425 000 долларов.

В ее жалобе утверждается, что компания знала, что ее кибербезопасность несовершенна, поскольку всего за несколько месяцев до фишинговых атак разработала план улучшения кибербезопасности. Проверка компании после атаки «признала, что ее нынешняя позиция в области кибербезопасности «отсутствует», — говорится в жалобе. Помимо отсутствия многофакторной аутентификации, в сети компании отсутствует система SIEM.

В соответствии с окончательным урегулированием коллективного иска каждое пострадавшее лицо имеет право на получение возмещения расходов в размере до 10 000 долларов США, включая документально подтвержденные невозмещенные наличные расходы, возникшие в результате инцидента с безопасностью, убытков от кражи личных данных и мошенничества, а также до 250 долларов США за время, потраченное на устранение проблем, связанных с нарушением.

Aveanna также согласилась обеспечить пять лет кражи личных данных и кредитного мониторинга.

Компания не сразу ответила на запрос Information Security Media Group о комментариях по принудительным действиям Хили и урегулированию коллективного иска». ***(Marianne Kolbasuk McGee. Aveanna Healthcare Data Breach Could Cost Firm More Than $1M // Information Security Media Group, Corp. (https://www.govinfosecurity.com/aveanna-healthcare-data-breach-could-cost-firm-more-than-1m-a-20428). 07.11.2022).***

***

«Сенатор Марк Уорнер предлагает ввести требования кибербезопасности через Medicare

Осуждая статус кибербезопасности в здравоохранении как проблему второго уровня, сенатор США предлагает, чтобы медицинские практики, участвующие в программе Medicare, подпадали под действие мандата на применение минимальных методов безопасности в качестве стандартной операционной процедуры.

Такой мандат будет иметь далеко идущие последствия для медицинской отрасли, учитывая значительную долю Medicare в расходах на здравоохранение в Соединенных Штатах — около 20 процентов, по оценкам правительства.

Предложение — оно не соответствует полностью одобренному предложению — содержится в отчете, опубликованном сенатором Марком Уорнером, демократом из Вирджинии, активно занимающимся технической политикой. «Переход к лучшей

кибербезопасности был болезненно медленным и неадекватным», — сказал он в своем заявлении.

Medicare уже налагает стандарты на участвующие практики, такие как меры по предотвращению распространения внутрибольничных инфекций или наличие источников аварийного питания.

«Многие заинтересованные стороны считают, что кибербезопасность так же важна, как и эти два примера, и что в эти правила следует включить некоторый минимальный уровень гигиены кибербезопасности», — говорится в отчете.

Medicare, в свою очередь, вероятно, должна определить, как включить затраты на кибербезопасность в формулы оплаты, добавляется в отчете.

Офис Warner ожидает комментариев к 1 декабря по предложенным в отчете вариантам политики с целью введения законодательства в следующие два года.

Дополнительные предложения по политике

Изменение условий участия и формулы оплаты Medicare — это лишь два из десятков предложений, содержащихся в отчете. Они включают:

Концепция кибербезопасности: разработка «консенсусной системы кибербезопасности для здравоохранения» может принять форму «профиля структуры», например, разработанного Национальным институтом стандартов и технологий для производственной и избирательной инфраструктуры, или, возможно, нового подраздела Текущая структура кибербезопасности NIST ориентирована на здравоохранение.

Модернизация HIPAA: обновление правил HIPAA для устранения более широкого круга угроз кибербезопасности вместо текущего акцента на ответственности регулируемых организаций по защите защищенной медицинской информации пациентов.

Закон Старка и Положение о борьбе с откатами: законодательное уточнение Закона Старка и Положения о борьбе с откатами, чтобы заинтересованные стороны организаций сектора здравоохранения знали, что им не мешают работать вместе над улучшением кибербезопасности.

Талант в области кибербезопасности: Конгресс учреждает программу развития рабочей силы, ориентированную на кибербезопасность здравоохранения.

Студенческие ссуды: предложение списания ссуды в качестве стимула для того, чтобы специалисты по кибербезопасности провели несколько лет, работая в сельской местности, аналогично Программе погашения ссуд Национальной службы здравоохранения.

Медицинские устройства: создайте стимулы для организаций здравоохранения, инвестирующих в системы, чтобы лучше отслеживать запасы своего медицинского оборудования или заменять устаревшее оборудование более новыми устройствами; ограничить продажу медицинских изделий с устаревшим программным обеспечением; требование спецификаций программного обеспечения для всего программного обеспечения и устройств, используемых в отрасли здравоохранения; Управление по санитарному надзору за качеством пищевых продуктов и медикаментов, требующее, чтобы медицинские устройства имели отказоустойчивый режим в случае сбоя подключения или других инцидентов безопасности.

Обмен информацией: Конгресс должен рассмотреть вопрос о создании «узко определенной» безопасной гавани для учреждений здравоохранения, которые обмениваются информацией об угрозах. В отчете говорится, что многие организации неохотно делятся информацией, опасаясь последствий, что препятствует принятию мер по смягчению последствий в реальном времени по всей отрасли.

Восстановление после кибератак: HHS может поручить медицинским учреждениям рассматривать кибератаки в той же категории, что и другие опасности, такие как ураганы и землетрясения, для процедур обеспечения готовности к чрезвычайным ситуациям; требование, чтобы весь медицинский персонал был обучен использованию альтернативных или устаревших систем в случае катастрофического отказа подключенных систем; создание программы помощи при стихийных бедствиях для жертв кибератак.

Национальный запас: пополнение национального запаса обычным оборудованием, необходимым больницам, сталкивающимся с кибератаками, включая аналогичные медицинские устройства, ноутбуки, рации и другие мобильные устройства.

Киберстрахование: создание федеральной программы перестрахования, которая покрывает планы, требующие минимальной кибергигиены; стандартизация элементов покрытия и стимулов для их внедрения страховыми компаниями; создание программы киберстрахования, аналогичной Закону о страховании террористических рисков, для создания прозрачной системы для определенных застрахованных убытков в результате кибератак национального государства; обязательную отчетность о выплатах по киберстрахованию.

Грег Гарсия, исполнительный директор Координационного совета сектора здравоохранения и общественного здравоохранения, государственно-частной группы, которая консультирует HHS по вопросам кибербезопасности, говорит, что сотрудники Warner проинформировали членов совета о предложениях.

Уорнер «права в том, что кибербезопасность — это безопасность пациентов», — говорит Гарсия.

Дениз Андерсон, президент и главный исполнительный директор Центра обмена и анализа медицинской информации, говорит, что новая политика кибербезопасности в сфере здравоохранения должна учитывать малый и средний бизнес.

«Финансовые стимулы, обучение и благоприятные нормативные послабления для обмена информацией об угрозах, уязвимостях и инцидентах — особенно автоматизированными способами — будут иметь большое значение для защиты всех организаций», — говорит она.

«Наиболее эффективными новыми законами и постановлениями будут те, которые будут способствовать сотрудничеству и раскрытию информации, а не налагать штрафы», — говорит юрист Эрик Вейник из юридической фирмы Otterbourg PC». ***(Marianne Kolbasuk McGee. Cybersecurity Is Patient Safety, Says US Senator // Information Security Media Group, Corp. (https://www.govinfosecurity.com/uk-ncsc-says-friendly-spooks-scanning-british-internet-a-20405). 03.11.2022).***

***

«…Согласно отчету комитета Конгресса, в 2021 году от кибератак на сектор здравоохранения пострадали 45 миллионов человек, что на 32% больше, чем годом ранее.

Председатель комитета сенатор Марк Уорнер, штат Вирджиния, сказал, что отрасль отстает в наращивании усилий в области кибербезопасности.

«К сожалению, сектор здравоохранения уникально уязвим для кибератак, а переход к лучшей кибербезопасности был мучительно медленным и неадекватным. Федеральное правительство и сектор здравоохранения должны найти сбалансированный подход к противодействию ужасным угрозам как партнеры с общей ответственностью»,- об этом Уорнер сообщил в пресс-релизе.

Кибератаки стали более частыми и во многих случаях более серьезными в нескольких отраслях, включая потребительские технологии и финансы. Комитет заявил, что кибератаки на сектор здравоохранения могут быть вопросом жизни и смерти.

В то время как медицинские работники сосредоточены на пациентах, хакеры могут представлять для них невидимую угрозу.

«Кибератаки могут нанести ущерб безопасности пациентов, поскольку они могут лишить врачей доступа к инструментам лечения, отключить больничное оборудование, используемое для ухода, и создать задержки, которые задерживают приемы и лечение».

Уорнер сказал, что федеральное правительство должно принять меры, чтобы помочь отрасли здравоохранения повысить стандарты кибербезопасности за счет финансирования, ресурсов и политических мандатов. Мандаты, вероятно, изменят будущее Закона о переносимости и подотчетности медицинского страхования, повысив защиту конфиденциальной информации пациентов.

Комитет также рекомендует правительству учредить программу перестрахования, чтобы помочь страховым компаниям возместить расходы, понесенные в результате кибератак. Страховые компании выплачивают все более крупные страховые взносы клиентам, которые регистрируются в страховом покрытии кибербезопасности.

«Личная медицинская информация на черном рынке более ценна, чем даже информация о кредитных картах, поскольку хакеры могут продавать украденные медицинские записи по цене от 10 до 1000 долларов за запись», — говорится в отчете». ***(Joe Fisher. Congressional committee warns of cyber security risks in healthcare sector // United Press International, Inc. (https://www.upi.com/Top_News/US/2022/11/03/8451667509159/). 03.11.2022).***

***

«Міжнародний Комітет Червоного Хреста запропонував створити цифровий еквівалент айдентики організації, щоби запобігти хакерським атакам на медзаклади по всьому світу. Про це пише Wall Street Journal.

«Цифрова емблема не лише забезпечуватиме технічний захист з кібербезпеки для лікарень, інфраструктури Червоного Хреста чи інших медичних закладів, але й

сигналізуватиме хакерам, що вони порушуватимуть міжнародне гуманітарне право», — заявив Тілман Роденхаузер, юридичний радник МЧХ.

Ще під час пандемії коронавірусу лікарні по всьому світу піддавалися зломам. Так чиказька компанія CommonSpirit Health, яка обслуговує понад 140 лікарень у 21 штаті США, була вражена програмою-вимагачем — це призвело до збоїв у роботі електронних медичних записів та у медичних картках пацієнтів. Після атаки програм-вимагачів у госпітальному центрі CHSF поблизу Парижа були перервані невідкладні операції - як наслідок, загинули пацієнти. Експерти зазначають, що хакери націлені на лікарні тому, що вони надають життєво важливі послуги, а отже — блискавично платять за відновлення своїх технологічних систем.

З лютого, коли росія з повномасштабною військовою агресією вдерлася на територію України, кілька постачальників медичних послуг також зазнали кібератак — про це повідомляє CyberPeace Institute. З лютого по жовтень в українських закладах охорони здоров'я сталися вже чотири такі інциденти, у тому числі три атаки на сайти лікарень. Жертвами зломів стали і п'ять естонських організацій, які надають підтримку Україні.

З метою запобігання небажаних кібервтручань аналітики Червоного Хреста запропонували впровадити такі цифрові символи: файл на кожному пристрої у всіх лікарнях організації та код, пов'язаний з IP-адресами медичних установ. Червоний Хрест та його кіберконсультанти працювали над цим проектом понад два роки…». ***(Для захисту від кібератак Червоний Хрест створить цифрову емблему // No worries! (https://noworries.news/dlya-zahystu-vid-kiberatak-chervonyj-hrest-stvoryt-czyfrovu-emblemu/). 07.11.2022).***

***

Захист персональних даних та соціальні мережі

«Компания урегулировала иск акционеров на 26 миллионов долларов

Компания SolarWinds, производитель программного обеспечения для управления сетью, которая была взломана российским правительством, теперь сталкивается с потенциальным расследованием Комиссии по ценным бумагам и биржам США в связи с раскрытием инцидента.

Хакеры из Службы внешней разведки России в начале 2020 года внедрили троянца в программу обновления программного обеспечения для флагманского приложения компании «Орион». По оценкам компании, заражение достигло менее 100 клиентов, в том числе не менее девяти федеральных агентств.

Компания из Остина, штат Техас, сообщила о возможном расследовании SEC в заявлении акционеров. Федеральные регулирующие органы приняли предварительное решение о том, что необходимо продолжить расследование того, нарушила ли компания закон о ценных бумагах, не раскрыв должным образом риски и инциденты кибербезопасности. Они отправили компании так называемое «уведомление Wells» — уведомление, которое не содержит формального обвинения

и позволяет компании оспорить предварительное решение персонала, что, по словам SolarWinds, она и сделает.

Если расследование будет продолжено, регулирующие органы могут заставить компанию заплатить гражданский штраф и пообещать улучшить контроль за раскрытием информации. SEC с 2011 года интерпретирует закон о ценных бумагах как обязывающий компании сообщать о рисках и инцидентах, и в 2018 году руководство было усилено. Критики говорят, что раскрытия информации, как правило, представляют собой шаблонные заявления, которые мало что говорят о реальных проблемах в киберпространстве. Ранее в этом году SEC предложила вторую редакцию, требующую текущей отчетности о существенных инцидентах кибербезопасности.

Потенциальное расследование начинается после того, как SolarWinds заявляет, что согласилась урегулировать предполагаемый коллективный иск акционеров в федеральном окружном суде Техаса на сумму 26 миллионов долларов. В сводной жалобе компания обвиняется в том, что она вводит инвесторов в заблуждение относительно надежности своей кибербезопасности, обвиняя ее в том, что она жертвует кибербезопасностью в пользу краткосрочной прибыли для двух своих основных частных инвесторов, Silver Lake Partners и Thoma Bravo.

Цена акций компании резко упала после того, как о взломе стало известно, и еще не восстановилась до уровня, существовавшего до инцидента. В иске ответчиками были названы компания, две частные инвестиционные компании и генеральный директор компании Кевин Томпсон и вице-президент по безопасности Тим Браун.

В марте федеральный судья отклонил жалобу на Томпсона, но постановил, что другие обвиняемые продолжат судебное разбирательство. Стороны подали в четверг уведомление, уведомляющее суд о достижении соглашения.

Компания, ее частные инвесторы и SEC не сразу ответили на запрос о комментариях». ***(David Perera. SolarWinds May Face SEC Investigation Over Hack Disclosure // Information Security Media Group, Corp. (https://www.govinfosecurity.com/solarwinds-may-face-sec-investigation-over-hack-disclosure-a-20416). 04.11.2022).***

***

«Сроки, истекающие в соответствии с приказом FTC США о согласии

Несколько СМИ сообщают, что старшие руководители Twitter, отвечающие за безопасность, конфиденциальность и соблюдение нормативных требований, уволились из компании, что ознаменовало эскалацию регулятивного воздействия на осажденную платформу социальных сетей и ее нового владельца Илона Маска.

Леа Кисснер, назначенная директором по информационной безопасности в январе, подтвердила их индивидуальную отставку, написав в Твиттере, что они приняли «тяжелое решение» покинуть компанию.

Директор по конфиденциальности Дэмиен Киран и директор по соблюдению требований Марианна Фогарти не сразу ответили на запросы о комментариях. «Я не смотрю «Игру престолов». Я определенно не хочу играть в нее на работе», —

написал Фогарти в Твиттере в понедельник, имея в виду сериал HBO, в котором несколько персонажей умирают, пытаясь получить власть.

Twitter был в беспорядке в течение 14 дней с тех пор, как самый богатый человек в мире Илон Маск вошел в офис Twitter в Сан-Франциско с раковиной после покупки компании за 44 миллиарда долларов. С тех пор Маск уволил примерно половину из 7500 сотрудников, отправил и удалил ссылку на теорию заговора, запускал и отключал функции продукта и угрожал «термоядерным именем и позором» рекламодателям, уходящим с платформы. Новая схема проверки Twitter привела к потоку проверенных, но на самом деле фальшивых учетных записей, таких как предполагаемая учетная запись бывшего президента США, вспоминающего: «Я скучаю по убийствам иракцев».

Хотя Twitter больше не торгуется публично, по закону он по-прежнему обязан назначить старшего сотрудника для решения вопросов кибербезопасности и конфиденциальности. В мае он подписал соглашение с Федеральной торговой комиссией США, обязывающее его поддерживать программу конфиденциальности и информационной безопасности в течение следующих двух десятилетий. Соглашение с Twitter положило конец расследованию использования Twitter телефонных номеров и адресов электронной почты в рекламных целях, когда они были собраны для использования в многофакторной аутентификации. Twitter также заплатил гражданский штраф в размере 150 миллионов долларов.

Среди требований программы - назначение «квалифицированного сотрудника или сотрудников для координации и ответственности» за программу.

Приказ также предписывает Twitter оценивать риски для конфиденциальности и безопасности, прежде чем вносить изменения в продукт и проводить ежегодные оценки своих средств контроля конфиденциальности и безопасности, а также сотрудничать с сторонними оценками, проводимыми раз в два года.

Компании грозит крайний срок 21 января 2023 года для подачи в агентство отчета, сделанного под страхом наказания за лжесвидетельство, подтверждающего выполнение заказа. По словам Меган Грей, бывшего юриста FTC и бывшего корпоративного юрисконсульта технологической компании, найти руководителя, готового подписать этот отчет, может быть проблематично. Руководители компании и, возможно, трио ушедших, вероятно, «больше не уверены, что компания будет выполнять юридические обязательства по отношению к ним лично», — сказала она.

Агентство «очень четко дало понять, что преследует руководителей», добавила она.

Представитель FTC сообщила Information Security Media Group, что агентство «с глубокой озабоченностью отслеживает последние события в Twitter. Ни один генеральный директор или компания не может быть выше закона, и компании должны следовать нашим указам о согласии».

Алекс Спиро, поверенный из ближайшего окружения Маска и новый глава юридического отдела в Twitter, как сообщается, не принимает во внимание возможность принудительного применения FTC, а внутреннее сообщение Slack цитирует его заявление: «Илон запускает ракеты в космос, он не боится FTC».

Twitter не ответил на запрос о комментарии». ***(David Parera. Twitter Ramps Up Regulatory Exposure After Loss of CISO // Information Security Media Group, Corp.***

(https://www.govinfosecurity.com/twitter-ramps-up-regulatory-exposure-after-loss-ciso-a-20445). 10.11.2022).

***

«Следователи установят, имел ли хакер доступ к информации о клиенте Legal Aid Group

Взлом австралийской группы юридической помощи на этой неделе, возможно, раскрыл личную информацию о домашнем насилии, жертвах сексуального насилия и других уязвимых людях в столице страны.

Legal Aid ACT, финансируемая государством независимая группа, которая предоставляет юридическую помощь по уголовным, семейным и гражданским делам, ориентированную на социально или экономически обездоленных, сообщила об атаке в четверг, заявив, что предприняла «быстрые действия» для защиты своих систем после обнаружения атаки. Legal Aid ACT наняла неназванную фирму по кибербезопасности для помощи в расследовании.

«На данном этапе мы не можем подтвердить, была ли затронута какая-либо информация о клиенте», — говорит Джон Бурсиг, генеральный директор Legal Aid ACT. Бурсиг говорит, что расследование продолжается и что некоторые системы и службы будут продолжать работать неопределенно долго, поскольку организация ужесточает меры безопасности и тщательно тестирует свои системы.

Legal AACT сообщает, что злоумышленник не связывался с ними и не получал никаких требований о выкупе. По словам Берсига, если будет получен доступ к какой-либо информации о клиенте, Legal Aid ACT свяжется с пострадавшими клиентами.

Группа, созданная в соответствии с Законом о правовой помощи 1977 года, предоставляет бесплатную юридическую помощь, включая юридическую информацию и консультации, услуги адвоката и финансовую помощь уязвимым и обездоленным лицам с ограниченным доступом к юридической помощи на территории столицы Австралии». ***(Mihir Bagwe. Sexual Assault, Abuse Victims' Data at Risk in Australia // Information Security Media Group, Corp. (https://www.govinfosecurity.com/sexual-assault-abuse-victims-data-at-risk-in-australia-a-20420). 04.11.2022).***

***

«Департамент офисных выговоров заявляет, что штраф составил бы более 10 миллионов фунтов стерлингов

Британский орган по надзору за данными объявил выговор правительственному агентству за разрешение несанкционированного использования базы данных, содержащей школьные записи подростков, фирмой, проверяющей возраст онлайн-игроков.

Управление Комиссара по информации заявляет, что Министерство образования нарушило закон о защите данных, когда разрешило компании Trustopia использовать базу данных для проверки возраста.

Расследование, спровоцированное разоблачениями доступа Trustopia, опубликованными The Sunday Times в 2020 году, показало, что департамент

предоставил 12 600 организациям доступ к базе данных национальной службы учебных записей. Это число теперь короче на 2600 и больше не включает Trustopia, объявило ICO в воскресенье.

Служба учебных записей содержит уникальные 10-значные номера учащихся и отслеживает учебные записи и квалификации учащихся в возрасте от 14 лет. Она содержит личную информацию до 28 миллионов детей и молодых людей.

Выговор не включает штраф, учитывая введенную в июне политику, освобождающую государственные учреждения от денежных штрафов на том основании, что штрафы сокращают услуги для граждан.

По словам комиссара по вопросам информации Джона Эдвардса, без такой политики штраф в размере чуть более 10 миллионов фунтов стерлингов был бы уместным.

В офисе говорят, что Министерство образования укрепило процесс регистрации для доступа к Службе учебных записей, но могло бы сделать больше для повышения его прозрачности.

Представитель департамента заявил в своем заявлении, что он тесно сотрудничал с офисом комиссара, чтобы предотвратить повторение злоупотреблений базой данных. «Мы очень серьезно относимся к безопасности данных, которые мы храним», — сказал представитель, пообещав дать более полный ответ в ближайшие месяцы.

В 2020 году тогдашний госсекретарь по образованию Гэвин Уильямсон сообщил парламенту, что инцидент произошел из-за того, что «образовательная учебная организация в нарушение своего соглашения с нами неправильно предоставила информацию об учащихся».

В офисе комиссара заявили, что Trustopia распалась в ходе расследования, поэтому принятие регулирующих мер против нее невозможно». ***(Akshaya Asokan. Using Student Data for Gambling Apps Is Bad, Says UK ICO // Information Security Media Group, Corp. (https://www.govinfosecurity.com/using-student-data-for-gambling-apps-bad-says-uk-ico-a-20427). 07.11.2022).***

***

«Облачная компания заявляет, что учетные записи пользователей не были взломаны, просто репозитории кода GitHub

Добавьте DropBox в список технологических компаний, переживающих многофакторный сбой. Во вторник компания по хранению и обмену файлами признала, что сотрудники попались на хорошо продуманную фишинговую кампанию, которая дала хакерам доступ к внутренним репозиториям кода и некоторой личной информации.

Хакеры не получили доступа к содержимому учетных записей облачного хранилища DropBox, паролям пользователей или их платежной информации, заявила компания из Сан-Франциско, штат Калифорния. Публичная компания сообщает о 700 миллионах зарегистрированных пользователей, из которых около 17 миллионов являются платными клиентами.

Вместо этого хакеры нашли и скопировали 130 репозиториев кода DropBox, хранящихся на GitHub, сообщает компания. Внутри репозиториев находились «наши

собственные копии сторонних библиотек, слегка модифицированные для использования в Dropbox, внутренние прототипы и некоторые инструменты и файлы конфигурации, используемые командой безопасности». Не был включен код для основных приложений или инфраструктуры, которые, по словам DropBox, контролируются более строгими уровнями безопасности.

В репозиториях были некоторые личные данные. «Код и связанные с ним данные также включали несколько тысяч имен и адресов электронной почты, принадлежащих сотрудникам Dropbox, текущим и прошлым клиентам, руководителям отдела продаж и поставщикам», — говорится в сообщении компании. DropBox заявляет, что уведомила пострадавших людей, несмотря на то что считает, что «любой риск для них минимален».

Признание взлома пришло после того, как несколько фирм Кремниевой долины недавно обнаружили, что их внутренняя безопасность не так защищена от хакеров, как считалось раньше.

Эксперты по безопасности уже давно рекомендуют многофакторную аутентификацию в качестве защиты от хакеров, пытающихся проникнуть в систему с помощью украденных или предполагаемых учетных данных. Злоумышленники приспосабливаются к этому совету, переключаясь на кражу учетных данных в реальном времени вместе с одноразовыми кодами аутентификации. Средствами являются фишинговые сообщения и точные копии законных сайтов входа.

Так было и с Dropbox. Злоумышленник попал в репозитории после отправки сотрудникам DropBox электронных писем, якобы отправленных с платформы разработки программного обеспечения CircleCl. Электронные письма, отправленные в начале октября, направляли кодировщиков DropBox на вредоносную страницу входа, имитирующую настоящую страницу входа CircleCl. Фишеры попросили кодеров ввести свои учетные данные GitHub, включая одноразовый пароль, сгенерированный с помощью аппаратного ключа аутентификации.

Фишинговая кампания была похожа на кампанию, о которой GitHub предупреждал пользователей в сентябре. Учетные записи, защищенные аппаратными ключами безопасности, не были уязвимы для обмана, даже если пользователи вводили учетные данные на поддельной странице входа в систему CircleCl.

DropBox заявляет, что инцидент подталкивает его к ускорению внутреннего внедрения стандарта аутентификации Web Authentication, формы многофакторного входа в систему, которая зависит от аутентификаторов, таких как небольшое USB-устройство». ***(David Parera. Dropbox Data Breach Another Multifactor Fail // Information Security Media Group, Corp. (https://www.govinfosecurity.com/dropbox-data-breach-another-multifactor-fail-a-20406). 03.11.2022).***

***

«Корреспондент Би-би-си по дезинформации и социальным сетям Марианна Спринг создала серию учетных записей в социальных сетях, чтобы выяснить, что избирателям рекомендуют онлайн в неспокойное для американской политики время. После более чем двух месяцев работы с профилями она нашла вот что.

Я открываю Instagram Бритни и нажимаю на аккаунт, рекомендованный в ее ленте. Меня приветствует мем, ложно заявляющий, что президент Джо Байден на самом деле никогда не выигрывал выборы 2020 года, и несколько других, нацеленных на женщин-политиков с женоненавистническими комментариями и оскорбительными выражениями.

Бритни — один из пяти профилей, которые я создал, чтобы отслеживать, что можно порекомендовать американским избирателям и что им показывать в Интернете в преддверии промежуточных выборов. В то время как сайты социальных сетей заявляют, что они привержены борьбе с дезинформацией и ненавистью на своих платформах в преддверии голосования, для моих избирателей, работающих под прикрытием, количество вводящих в заблуждение и насильственных сообщений, похоже, только увеличилось за последние недели…» ***(BBC Voter Profiles Shown Hate and Disinformation Online // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/bbc-voter-profiles-shown-hate-and-disinformation-online/). 12.11.2022).***

***

«Регуляторное агентство является последней организацией, которая предложила свои собственные требования к конфиденциальности данных потребителей, отсутствующие в всеобъемлющем федеральном законе.

Бюро финансовой защиты потребителей предпринимает шаги, чтобы потенциально включить больше правил защиты финансовых данных в федеральные правила, чтобы помочь людям сохранить контроль над своей конфиденциальной информацией.

CFPB, изложенный в серии новых предложений, в настоящее время принимает отзывы о предложенных правилах по внесению поправок в Закон Додда-Франка о реформе Уолл-стрит и защите прав потребителей, которые направлены на усиление контроля потребителей и их знаний о своих финансовых данных в бизнес-операциях компаний.

Чиновники CFPB объявили о новых предлагаемых правилах, дополняющих раздел 1033(а) Закона Додда-Франка 27 октября. Они охватывают такие области регулирования, как хранение записей, получение информации и раскрытие информации клиентам от уполномоченных третьих лиц.

«Доминирующие фирмы не должны иметь возможности накапливать наши личные данные и присваивать себе ценность», — сказал директор CFPB Рохит Чопра. «Нормотворчество CFPB в области прав на личные финансовые данные может дать толчок конкуренции, предоставив американцам новые возможности для финансовых продуктов».

Агентство разработало предложения на основе собственного анализа, а также на основе отзывов общественности, в частности, собранных в рамках предварительного уведомления CFPB о предлагаемом нормотворчестве в отношении доступа к данным потребителей от 2020 года.

Это нормотворчество заставит частные компании улучшать свои услуги и продукты для передачи данных, чтобы они лучше соответствовали безопасности потребителей, а также давало потребителям больше возможностей отказаться от

определенных услуг. К компаниям, на которые распространяются эти правила, относятся банки и депозитарные учреждения, финансовые технологические компании и любые другие фирмы, которые собирают и хранят пользовательские данные.

В соответствии с Законом о справедливости регулирования малого бизнеса, CFPB должен будет созвать Группу по рассмотрению вопросов малого бизнеса для оценки экономического воздействия предлагаемых правил на предприятия, которые обрабатывают финансовые данные. Эта группа будет состоять из одного представителя от Управления по защите интересов малого бизнеса, одного представителя от Управления информации и регулирования в Управлении по вопросам управления и бюджета и одного представителя от CFPB.

В течение 60 дней после созыва комиссия представит в открытый доступ отчет о нормотворчестве, состоящий из рекомендаций опрошенных представителей малых предприятий, на которых, вероятно, повлияют предлагаемые дополнения к Закону Додда-Франка. Затем CFPB примет во внимание эту обратную связь.

Нормотворчество CFPB — это последняя федеральная попытка усилить защиту потребителей и контроль над индивидуальными данными. В отсутствие федерального закона о конфиденциальности данных такие агентства, как CFPB и Федеральная торговая комиссия, недавно разработали свои собственные правила и полномочия, касающиеся конфиденциальности данных потребителей.

Ранее на этой неделе Чопра открыл заседание Консультативного совета CFPB заявлением, в котором подчеркиваются права на финансовые данные и предстоящие действия агентства по защите конфиденциальных данных в рамках поворота к более открытому банковскому обслуживанию в США». ***(Alexandra Kelley. The regulatory agency is the latest entity to propose its own consumer data privacy requirements absent an overarching federal law // Nextgov (https://www.nextgov.com/analytics-data/2022/11/cfpb-targets-financial-industrys-ability-hoard-personal-data-proposed-rule/379362/). 04.11.2022).***

***

«Первая политика Министерства обороны в отношении социальных сетей, DoDI 5400.17, является началом, но имеет существенные недостатки.

Министерство обороны особенно уязвимо для компрометации через социальные сети. Несмотря на инциденты с Робином Сейджем, захватом и искажением официальной учетной записи в Твиттере, посвященной инцидентам Центрального командования США, Министерство обороны не спешило формализовать общеведомственную политику в отношении официального и личного использования социальных сетей. Тем временем субъекты угрозы, от мошенников низкого уровня до иностранных разведывательных структур, злоупотребляют американскими социальными сетями для финансовых преступлений и шпионажа. Из-за этих двух и многих других инцидентов Министерство обороны, наконец, разработало общеведомственную политику в отношении социальных сетей, Инструкцию Министерства обороны 5400.17, касающуюся как внешнего официального присутствия (EOP), так и личного использования социальных сетей персоналом Министерства обороны.

За последний год аналитики ZeroFox в области разведки угроз наблюдали значительное увеличение как числа целей, так и финансовых потерь из-за того, что ФБР придумало мошенничество «доверие/романтика» — тип мошенничества в более широкой категории «социальной инженерии». Эти мошенники используют военную форму как символ доверия, чтобы играть на человеческих эмоциях, либо для развития романтических отношений с гражданскими жертвами, либо для того, чтобы заманить военнослужащих в отношения, используя поддельные профили знакомств. Неудивительно, что преступники без колебаний используют умерших солдат. Мы отслеживаем мошенников, выдающих себя за обладателя Почетной медали, который, к сожалению, умер от рака, лоббируя законодательные изменения в Конгрессе. Еще один показатель, демонстрирующий масштабы проблемы — известно, что ныне отставной четырехзвездный генерал выдавал себя за него 52000 раз в социальных сетях — наибольшее количество пародий на одного человека, отслеженных ZeroFox на сегодняшний день. Только 15 000 из этих случаев произошли, когда генерал находился на действительной службе.

Мошенничество в романтических отношениях, нацеленное на военнослужащих США и их семьи, растет с экспоненциальной скоростью. С 2018 года военнослужащие подали более 700 000 отчетов в книгу данных FTC Consumer Sentinel Network Data Book за 2021 год. Общие убытки составили 718,7 млн долларов, что почти вдвое превышает сумму, указанную за четырехлетний период в книге данных за 2020 год. Фактические инциденты и потери, вероятно, на порядок выше, поскольку большинство жертв не сообщают об этих преступлениях. С точки зрения национальной безопасности эта статистика должна стать тревожным звонком. Масштабы мошенничества с военными романами подрывают доверие к вооруженным силам США и снижают боеготовность в то время, когда наша конкуренция как с Россией, так и с Китаем находится на пике за последние десятилетия.

Мошенничество с романтикой и доверием — не единственная цель злоумышленников в социальных сетях. В августе неизвестный злоумышленник скопировал текст официального поста армии США, касающегося IPPS-A — новой интегрированной армейской системы оплаты труда и кадров — и разместил его под фальшивым профилем действующего генерала с четырьмя звездами, но изменил адрес электронной почты. адрес с Army.mil на gmail.com. Мы можем сделать вывод, что целью злоумышленника, ответственного за выдачу себя за другое лицо, было украсть персональные данные солдат армии США, но с какой целью — с целью получения финансовой выгоды или шпионажа?

Если бы этот пост был частью шпионской кампании, это был бы не первый случай, когда иностранная разведка создала профиль в социальной сети, выдавая себя за чиновника Министерства обороны. В деле бывшего агента контрразведки ВВС США Моники Уитт о дезертирстве и шпионаже ее иранские сообщники создали профиль, выдававший себя за сотрудника Министерства обороны США, и использовали этот фальшивый профиль для нападения на других сотрудников Министерства обороны, имеющих доступ к информации о национальной безопасности.

Руководители всех эшелонов должны быть первыми в использовании социальных сетей. Военные лидеры, как правило, стесняются социальных сетей по очевидным причинам OPSEC. Однако вооруженные силы США должны рассказать свою историю, иначе ее расскажет кто-то другой. Большему количеству подразделений и лидеров необходимо создать официальные и проверенные профили в социальных сетях. Опередить угрозы может быть так же просто, как установить свое присутствие до того, как они сделают это за вас.

Это не означает, что все, кому платят за ношение униформы, должны использовать фотографии «крутых парней» в качестве своих аватарок. Если человек не использует социальные сети официальным образом в соответствии с руководством EOP, все военнослужащие должны воздерживаться от фотографий профиля в форме или использования титулов и званий в своих профилях. Другие фотографии и сообщения должны быть сделаны со строгим контролем конфиденциальности, чтобы ограничить возможности мошенников поднимать и перемещать контент в поддельный профиль или просматривать сообщения, которые могут повлиять на OPSEC. Лидеры должны демонстрировать ответственное использование социальных сетей, присутствуя там, где находятся члены их подразделения, и отговаривать их от публикации информации о допуске к безопасности.

Министерство обороны также должно обновить политику, чтобы обязать официальных менеджеров социальных сетей для EOP использовать многофакторную аутентификацию и уникальный пароль для предотвращения захвата учетной записи. Текущая версия DODI 5400.17 не требует каких-либо специальных мер безопасности для официальных учетных записей социальных сетей. Эти стандартные меры безопасности необходимы для предотвращения таких инцидентов, как захват учетной записи CENTCOM в Twitter.

Министерству обороны следует создать новую инструкцию, которая устраняет разрыв между 5400.17 и O-2000.22 (Обозначение и физическая защита персонала Министерства обороны с высоким риском), которая сосредоточена исключительно на защите цифровых персон. Новая инструкция будет предназначена для защиты цифровых личностей назначенных высокопоставленных отдельных военнослужащих, политических назначенцев, награжденных Почетной медалью и других военнослужащих, чьи изображения, как известно, подвергались злоупотреблениям.

Фальшивые аккаунты в социальных сетях были проблемой в течение многих лет. Инвесторы, рекламодатели и политики должны подталкивать социальные сети к выявлению вероятных поддельных и спам-аккаунтов и предупреждать любых лиц, выдающих себя за них. Честность на этих платформах имеет решающее значение для укрепления доверия со стороны инвесторов, рекламодателей и политиков.

На данный момент Вооруженные силы США являются самой надежной организацией в США. Это доверие окажется под угрозой, если министерство обороны не сможет справиться с рисками, связанными с социальными сетями, такими как захват учетных записей и выдача себя за другое лицо. У Министерства обороны также есть потрясающая возможность улучшить свой имидж и расширить

круг претендентов. Лидеры всех уровней также являются ключом к успеху на полях сражений в социальных сетях.

Взгляды, выраженные здесь, принадлежат автору и не обязательно поддерживаются организацией Homeland Security Today, которая приветствует широкий спектр точек зрения в поддержку обеспечения безопасности нашей родины. Чтобы отправить статью на рассмотрение, напишите по адресу Editor@Hstoday.us». ***(Brian Kime. PERSPECTIVE: Military Leaders Must Lead from the Front on Social Media's Strategic Opportunities and Risks // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/perspective-military-leaders-must-lead-from-the-front-on-social-medias-strategic-opportunities-and-risks/). 08.11.2022).***

***

«…Компанія Google погодилася заплатити $391,5 млн, щоб врегулювати позов, який пов'язаний із незаконним збором даних користувачів. Про це пише Associated Press.

Позов до Google подали 40 американських штатів. Розслідування спровокувала публікація Associated Press 2018 року. Тоді журналісти виявили, що Google продовжувала відстежувати дані про місцезнаходження людей навіть після того, як вони вимкнули цю функцію.

Генеральні прокурори назвали угоду історичною перемогою для споживачів і найбільшою міжштатною угодою в історії США щодо конфіденційності.

«Дані про місцезнаходження є одними з найбільш конфіденційних і цінних особистих даних, які Google збирає. Є багато причин, чому споживач може відмовитися від відстеження», — заявив генеральний прокурор Коннектикуту Вільям Тонг.

Він закликав користувачів провести особисту інвентаризацію своїх онлайн-налаштувань і за потреби вимкнути їх.

«Не буде перебільшенням сказати, що ми живемо в економіці спостереження. Зрозумійте, що за вами стежать кожну хвилину кожного дня, де ви знаходитесь», — зазначив Тонг.

Компанія Google заявила, що вирішила проблеми із відстеженням місцезнаходження кілька років тому.

«Відповідно до вдосконалень, які ми внесли за останні роки, ми завершили це розслідування. Воно ґрунтувалося на застарілих підходах до продуктів, які ми змінили кілька років тому», — розповів речник компанії Хосе Кастанеда.

Прокурори заявили, що Google вводила користувачів в оману щодо своєї практики відстеження місцезнаходження принаймні з 2014 року, порушуючи закони штату про захист прав споживачів.

У результаті Google погодилася зробити цю практику більш прозорою. Зокрема, показувати більше інформації для контролю даних, які збирає…». ***(Google заплатить понад $390 млн через претензії щодо відстеження місцезнаходження користувачів // ДМ media sapiens (https://ms.detector.media/kiberbezpeka/post/30671/2022-11-15-google-zaplatyt-ponad-***

390-mln-cherez-pretenzii-shchodo-vidstezhennya-mistseznakhodzhennya-korystuvachiv/). 15.11.2022).

***

«Google согласился на урегулирование иска, поданного большинством генеральных прокуроров штатов США, и должен выплатить штраф в размере 391,5 миллиона долларов, а также повысить прозрачность для потребителей в отношении того, как и когда он участвует в отслеживании местоположения.

Инициированный Орегоном и Небраской, иск в конечном итоге включал 40 штатов и был сосредоточен на средствах, с помощью которых компания поддерживает отслеживание местоположения для отдельных приложений даже после того, как пользователи Android отказались от этого в своих глобальных настройках. Компания недавно урегулировала очень похожий иск, поданный в Аризоне, в котором она согласилась на отдельный платеж в размере 85 миллионов долларов.

Практика отслеживания местоположения Google по-прежнему влечет за собой финансовые санкции на уровне штата.

Android предоставляет настройки на уровне ОС, которые позволяют пользователям отказаться от любого отслеживания местоположения при использовании устройств, но серия судебных исков показала, что некоторые приложения и функции продолжают регистрировать и отслеживать пользователей, даже когда эти настройки задействованы.

В дополнение к расчетной сумме Google теперь потребуется создать специальную веб-страницу, которая информирует пользователей о различных ситуациях, в которых он собирает данные отслеживания местоположения, даже если включены настройки конфиденциальности. Также требовалось внести ряд улучшений прозрачности операционной системы и приложений для конечного пользователя, что описано в недавнем сообщении в блоге. К ним относятся дополнительные раскрытия, добавленные к элементам управления активностью, создание центрального «информационного узла», более простые средства для удаления сохраненных данных о местоположении (включая автоматическое удаление данных по истечении заданного времени) и более подробные пояснения об отслеживании местоположения во время новых событий. настройка аккаунта. Google говорит, что эти улучшения отслеживания местоположения будут внедрены в «ближайшие месяцы».

Дело началось с расследования, возбужденного рядом генеральных прокуроров штатов в 2018 году в ответ на жалобы потребителей. Расследование показало, что Google вводил в заблуждение относительно использования отслеживания местоположения по крайней мере с 2014 года и нарушал законы о защите прав потребителей. Отслеживание местоположения снова стало деликатной темой интереса в США после отмены дела Роу против Уэйда, что вызвало широко распространенные опасения, что штаты, в которых аборты запрещены, будут использовать записи из Google и аналогичных служб для судебного преследования. Google уже заявил, что намерен автоматически удалять записи о посещении особо секретных мест, таких как клиники для абортов.

Джейсон Хикс, полевой директор по информационным технологиям и исполнительный советник Coalfire, отмечает, что основная проблема, представленная в этом случае, заключается в том, что параметры конфиденциальности часто запутаны, а не просто отсутствуют: «Учитывая очень частный характер данных о местоположении, для производителей устройств и программного обеспечения важно обеспечить возможности, предоставляемые потребителям для управления отслеживание этих данных легко понять и работает так, как ожидалось. Если потребители как группа начнут сомневаться в своей способности включать и отключать отслеживание местоположения с помощью приложения или службы, вероятно, многие просто решат полностью отключить его. Это был бы наихудший сценарий для технологической компании, учитывая размер дохода, который они получают от рекламы на основе местоположения. Есть много случаев использования, когда некоторым людям будет удобно разрешить отслеживание данных о местоположении, при условии, что их выбор в отношении отказа соблюдается.

Доходы от иска будут разделены между штатами, при этом самые большие суммы пойдут Орегону (14,8 млн долларов) и Небраске (11,8 млн долларов) за их ведущую роль в разработке дела. Выручка обычно направляется в государственные «общие фонды», используемые для различных программ.

Некоторые приложения Google, функции сохранялись в отслеживании местоположения, несмотря на настройки конфиденциальности.

Одной из функций, упомянутых в иске, является компонент «Активность в Интернете и приложениях» учетных записей Google и устройств Android, который можно найти в меню настроек. Отключение этого параметра должно помешать Google собирать какие-либо новые данные отслеживания местоположения, но расследование показало, что он продолжал собирать определенную информацию даже после отключения. Это было использовано для информирования его целевой рекламной программы.

В судебных исках штата также отмечаются расследования, которые показали, что некоторые приложения всегда регистрируют информацию о местоположении пользователя с отметкой времени, даже если включены настройки конфиденциальности Android. В некоторых случаях, например с функцией временной шкалы Google Maps, можно отключить эту регистрацию из приложения, но за счет определенных функций (например, использование приложений для совместного использования).

В дополнение к множеству судебных исков по отслеживанию местоположения со стороны большинства штатов, Комитет Палаты представителей по энергетике и торговле ранее задавал вопросы Apple и Alphabet, материнской компании Google, о том, как они защищают конфиденциальность пользователей. 16-месячное расследование, завершившееся в конце 2020 года, показало, что эти компании, наряду с другими технологическими гигантами, такими как Facebook, использовали огромное количество персональных данных, которые они собирают, для создания монополий, хотя этот вывод еще предстоит воплотить в значимых действиях. Другие технологические гиганты также столкнулись с судебными исками, связанными с тайным вторжением в частную жизнь: Facebook недавно урегулировал иск в

Калифорнии на 37,5 миллионов долларов, в котором его приложение продолжало отслеживать пользователей, даже когда оно должно было быть ограничено настройками ОС.

Проблемы с отслеживанием местоположения для технологических гигантов также далеко не ограничиваются границами США; аналогичные проблемы были основанием для дела, которое Google проиграл в Федеральном суде Австралии в 2021 году, и он подал ряд жалоб на конфиденциальность в ЕС в соответствии со строгими законами о конфиденциальности данных (и был первым из технологических гигантов, которые столкнулись с серьезный штраф за конфиденциальность). Тем не менее, с годовым доходом от рекламы Alphabet, превышающим 1 миллиард долларов, возможно, просто решила, что случайные судебные решения такого типа являются приемлемыми затратами на ведение бизнеса.

Крис Маклеллан, операционный директор некоммерческой организации Data Collaboration Alliance, считает, что потребуются гораздо более решительные юридические действия, прежде чем пользователи смогут ожидать, что эти приложения будут полностью уважать их конфиденциальность: и игра с мышью, где потребитель всегда проигрывает. На сегодняшний день мы видим, что крупные штрафы ничего не изменили. И эти компании могут позволить себе оплачивать штрафы как расходы на ведение бизнеса».

«Штрафы — это не ответ. Нам необходимо стремиться к поощрению использования новых технологий, стандартов и методологий, которые помогают в первую очередь устранить коренные причины хаоса данных — разрозненность и копии. То, как будут развиваться права на данные и право собственности на данные, определит победителей и проигравших в нашей будущей экономике. Сейчас мы являемся свидетелями борьбы за будущее, владея данными», — добавил Маклеллан.

Клод Мэнди, главный евангелист отдела безопасности данных в Symmetry Systems, отмечает, что компании, у которых нет таких глубоких карманов, как у Google, также должны обратить внимание на эти решения: «Это соглашение является еще одним примером того, что регулирующие органы все больше внимания уделяют не только проверке поле соответствия, но больше о том, как выбор конфиденциальности зависит от пользовательского опыта и дизайна. Все организации должны использовать это как толчок, чтобы взглянуть на свои собственные методы и заранее упростить любые конфликтующие варианты и упростить выбор вариантов повышения конфиденциальности для своих клиентов. Как только эти аспекты будут реализованы, организации смогут обеспечить безопасную обработку данных в соответствии с выбором конфиденциальности своих клиентов». ***(Scott Ikeda. Google Agrees to $391 Million Payment To Settle Multi-State Location Tracking Lawsuit // CPO Magazine (https://www.cpomagazine.com/data-protection/google-agrees-to-391-million-payment-to-settle-multi-state-location-tracking-lawsuit/). 18.11.2022).***

***

«Система утечек данных, длившаяся четыре года и приписываемая Федеральной торговой комиссии (FTC) «небрежности», привела к тому, что у гиганта образовательных технологий Чегга возникли проблемы с законом.

FTC подала жалобу, в которой упоминаются четыре утечки данных, которые произошли в период с 2017 по 2020 год, что привело к краже 40 миллионов записей о клиентах. Агентство связывает эти инциденты с плохой практикой безопасности, в том числе с общими логинами сотрудников и хранением данных в открытом виде. Жалоба включает в себя приказы Chegg (и, соответственно, индустрии образовательных технологий) настроить свою программу безопасности данных и обеспечить, чтобы клиенты имели доступ к своим сохраненным данным.

Сбои в системе безопасности Chegg повышают ожидания индустрии образовательных технологий

Чегг работает с 2005 года и предлагает различные услуги в области образовательных технологий, включая аренду учебников и онлайн-репетиторство. Компания продемонстрировала огромный рост в 2020 и 2021 годах из-за мер по борьбе с пандемией Covid-19, из-за которых большинство студентов работали из дома. Но расследование FTC показывает, что методы кибербезопасности компании уже давно недостаточны для защиты собираемых конфиденциальных данных.

Нынешние юридические проблемы Чегга возникли примерно за четыре года до пандемии. С 2017 по 2020 год компания столкнулась с четырьмя серьезными утечками данных, и FTC считает, что это было не просто чередой неудач, а скорее повсеместным отсутствием заботы о кибербезопасности и безопасном обращении с пользовательскими данными.

В дополнение к сбору информации о платежах, различные службы образовательного гиганта (в частности, его служба поиска стипендий) также собирали различные категории конфиденциальной личной информации, к которой у предприятий часто нет доступа: информация об инвалидности, дата рождения, доход семьи, религиозная принадлежность и т. д. более. Компания использовала AWS S3 для хранения всей этой информации, но, как сообщается, предоставила всем своим сторонним подрядчикам доступ к ней с полными административными привилегиями с использованием одного ключа доступа. Сообщается, что данные сотрудников, хранящиеся в открытом виде, включая номера социального страхования и банковскую информацию, также подвергались риску.

Безрассудное использование AWS S3 было далеко не единственной неудачей, доставившей неприятности Чеггу. Жалоба FTC выглядит как подробный список неэффективных методов кибербезопасности, на которые направлено обычное обучение сотрудников. Компания не шифровала свои хранимые данные, не предъявляла никаких требований к многофакторной аутентификации, использовала устаревшую и небезопасную криптографическую функцию MD5 для защиты паролей пользователей до 2018 года, до 2020 года не проводила обучения сотрудников или подрядчиков по безопасности, не имел каких-либо формальных политик кибербезопасности до 2021 года, не проводил надлежащую инвентаризацию и удаление устаревшей личной информации, которую он хранил, и не отслеживал внутреннюю сеть на предмет несанкционированной кражи личной информации.

Большинство утечек данных edtech были связаны с фишингом, но мошенник, бывший сотрудник подрядчика, заметил эту очень слабую внутреннюю безопасность в 2018 году и воспользовался ею, чтобы украсть 40 миллионов файлов, полных текстовых данных и паролей, защищенных только MD5. Чегг раздавал свои учетные данные AWS Root Credential подрядчикам, несмотря на то, что Amazon предупреждала всех клиентов, что с ними следует обращаться как с «номером кредитной карты» или аналогичной конфиденциальной информацией. Федеральная торговая комиссия также обнаружила, что если бы в то время у компании был надлежащий мониторинг безопасности, она бы заметила кражу файлов. Позже в 2018 году Чегг был уведомлен о том, что взломанные пароли были найдены для продажи в даркнете, но компания продолжала хранить информацию о клиентах в открытом виде в своих учетных записях S3.

Первый из фишинговых инцидентов, приведших к утечке данных, произошел в 2017 году, когда была взломана учетная запись сотрудника, и злоумышленники смогли получить доступ к информации о прямом депозите отдела заработной платы. Федеральная торговая комиссия обнаружила, что в то время компания не проводила соответствующих тренингов по безопасности для сотрудников. В 2019 году высокопоставленный руководитель Chegg подвергся фишингу, что привело к компрометации всей системы электронной почты компании, которая была настроена на обход MFA, чтобы обеспечить более удобный доступ сотрудников. А в 2020 году старший сотрудник по расчету заработной платы был взломан, в результате чего была украдена налоговая информация примерно о 700 нынешних и бывших сотрудниках компании edtech. FTC обнаружила, что обучение безопасности не было обновлено для решения этих проблем после их возникновения.

Последовательность утечек данных требует обязательных улучшений безопасности

Чегг урегулировал жалобу, и приказ FTC требует, чтобы гигант образовательных технологий реструктурировал свою программу защиты данных. Он также должен следовать графику сбора личной информации и уведомления субъектов данных о том, как она используется, а также должен предоставлять доступ к сохраненным данным и возможность запрашивать удаление. И клиентам, и сотрудникам должны быть предоставлены варианты входа в систему с двухфакторной аутентификацией. Нарушения этих приказов могут повлечь за собой штрафы в размере до 46 517 долларов США за каждый инцидент, но урегулирование позволяет компании избежать немедленных финансовых санкций.

Судебный иск, по-видимому, является частью более широкой борьбы с ненадлежащей практикой в индустрии образовательных технологий; В мае FTC выпустила служебную записку, в которой указывалось, что она нацелена на отрасль из-за жалоб на обработку данных студентов и чрезмерный сбор. Однако в последнее время были предприняты действия против различных отраслей промышленности, и за аналогичные проблемы были наложены серьезные штрафы на Uber и приложение для доставки алкоголя Drizly.

Джо Гарбер, директор по маркетингу в Axiad, считает, что этого, вероятно, недостаточно, чтобы решить проблемы безопасности компании в ближайшем будущем: «Эта новость — еще один пример того, как организация не была

достаточно подготовлена к кибератаке на основе личных данных, а затем расплачивается за это. В данном случае тревожные сигналы, безусловно, были видны, так как за последние три года было четыре нарушения, а значит, последнее можно было предотвратить. Требование Федеральной торговой комиссией США (FTC) конкретных изменений в системе кибербезопасности организации имеет логичный смысл в этом контексте, особенно действия, необходимые для лучшей защиты учетных записей пользователей. Однако полномочий на простое внедрение MFA, вероятно, недостаточно, учитывая то, что организация неоднократно подвергалась фишинговым атакам. Важно знать, что не все МФА одинаковы, и злоумышленники часто могут нарушить процесс аутентификации — часто путем кражи учетных данных пользователей через поддельные страницы входа — с меньшими возможностями. MFA, усиленный методами защиты от фишинга, такими как FIDO2 и проверка подлинности на основе сертификатов (CBA), а также использованием надежных аппаратных токенов и соответствием таким стандартам, как проверка поведения пользователя, обеспечивает самый надежный уровень защиты от фишинговых атак. Такой подход, казалось бы, был бы уместным в данной ситуации». обеспечивают самый надежный уровень защиты от фишинговых атак. Такой подход, казалось бы, был бы уместным в данной ситуации». обеспечивают самый надежный уровень защиты от фишинговых атак. Такой подход, казалось бы, был бы уместным в данной ситуации». ***(Scott Ikeda. FTC Takes Legal Action Against Edtech Outfit Chegg Over Years-long String of Data Breaches // CPO Magazine (https://www.cpomagazine.com/cyber-security/ftc-takes-legal-action-against-edtech-outfit-chegg-over-years-long-string-of-data-breaches/). 09.11.2022).***

***

«Компания Bed, Bath & Beyond подтвердила утечку данных в результате целенаправленной фишинговой атаки на одного из своих сотрудников.

В октябре 2022 года крупный розничный продавец заметил, что третья сторона неправомерно получила доступ к его данным после успешного фишингового мошенничества со стороны неназванного злоумышленника. Злоумышленник получил доступ к данным на жестком диске сотрудника и общим дискам, к которым сотрудник мог получить доступ.

Bed, Bath & Beyond, имеющая торговые точки в 950 точках в США, Канаде, Мексике и Пуэрто-Рико, входит в список Fortune 500 с рыночной капитализацией около 0,35 млрд долларов и выручкой 7,87 млрд долларов в 2022 году.

Beth, Bath & Beyond изучают возможную утечку информации после фишинговой атаки

Bed Bath & Beyond заявила, что изучает утечку данных, чтобы определить, не содержалась ли на дисках какая-либо конфиденциальная информация.

«Компания просматривает полученные данные, чтобы определить, содержат ли эти диски какую-либо конфиденциальную и/или личную информацию», — заявила компания в своем заявлении 8K в Комиссию по ценным бумагам и биржам США.

Тем не менее, Bed, Bath & Beyond считает, что во время фишинговой атаки не было доступа к конфиденциальной или личной информации. Кроме того, розничный

гигант прогнозирует, что инцидент с кибербезопасностью не окажет существенного влияния на компанию.

«В настоящее время у Компании нет оснований полагать, что был получен доступ к такой конфиденциальной или личной информации или что это событие может оказать существенное влияние на Компанию».

Bed, Bath & Beyond очень скупы на детали и не предоставили больше информации о фишинговой атаке. Компания также не оценила количество клиентов, пострадавших от утечки данных.

За раскрытием информации последовало объявление о запланированном уходе клиента и технического директора компании Рафеха Масуда 2 декабря 2022 года. Однако уход Масуда, похоже, не связан с недавней утечкой данных или какими-либо событиями в компании.

Арти Раман, генеральный директор и основатель Titaniam, призвал к сочувствию, указав, что фишинговая атака может затронуть любую организацию.

«Фишинговая атака может случиться с каждым из нас, и есть статистика, подтверждающая это. Данные показывают, что на фишинг приходится около 90% утечек данных. Поэтому первая реакция, которую мы должны получить как сообщество, — это сочувствие жертвам».

Она рекомендовала инвестировать в обучение по борьбе с фишингом, чтобы сотрудники «были в курсе вопросов безопасности».

«ИТ-администраторам настоятельно рекомендуется постоянное обучение по вопросам безопасности и имитация фишинга для сотрудников, чтобы держать безопасность в центре внимания во всей организации».

Раман также рекомендовал «используемое шифрование данных», чтобы киберпреступники не могли злоупотреблять украденными данными после успешного взлома данных.

«Используемое шифрование уже используется ведущими предприятиями для защиты как структурированных, так и неструктурированных данных в облачных, локальных и гибридных средах», — сказала она. «Он доступен для современных облачных сред, а также для устаревшей инфраструктуры и помогает нейтрализовать все возможные рычаги, связанные с данными, и значительно ограничивает влияние раскрытия данных, программ-вымогателей и / или взлома».

Тим Прендергаст, генеральный директор strongDM, сказал, что фишинг был «средством до конца» для каждого киберпреступника, надеющегося получить доступ к неправильно сохраненным учетным данным, потому что они являются «VIP-пропусками в базы данных и серверы».

«После того, как злоумышленники получают эти действительные учетные данные, они часто получают неограниченный внутренний доступ. Вместо того, чтобы указывать пальцем, потому что на самом деле это могло случиться с каждым, директорам по информационной безопасности важно переоценить видимость и контроль доступа как к приложениям, так и к инфраструктуре».

Вторая утечка данных за три года

Этот инцидент знаменует собой второй случай, когда компания Bed, Bath & Beyond сообщает об утечке данных после того, как в 2019 году в результате атаки с

заполнением учетных данных было скомпрометировано менее 1% учетных записей ее клиентов.

По данным компании, хакеры получили имена пользователей и пароли в результате утечки внешних данных и полагались на повторное использование паролей пользователей для взлома учетных записей Bed, Bath & Beyond. 29 октября 2019 г. компания Bed, Bath & Beyond начала уведомлять клиентов и наняла фирму, занимающуюся киберкриминалистикой, для расследования инцидента.

Тем не менее, в 2019 году ритейлер товаров для дома сообщил, что сотрудник колл-центра, ответственный за обработку телефонных заказов, мог попытаться взломать кредитные карты клиентов.

Компания уволила сотрудника, сообщила об инциденте в правоохранительные органы и уведомила финансовые учреждения и держателей карт». ***(Alicia Hope. Bed, Bath & Beyond Confirms a Data Breach From Targeted Phishing Attack // CPO Magazine (https://www.cpomagazine.com/cyber-security/bed-bath-beyond-confirms-a-data-breach-from-targeted-phishing-attack/). 09.11.2022).***

***

«Обновление политики конфиденциальности компании теперь ясно дает понять, что пользовательские данные TikTok, собранные в Европе, становятся доступными для сотрудников в Китае на фоне расследования Ирландской комиссии по защите данных (DPC) о том, соответствует ли его передача данных стандарту, установленному General Data. Регламент защиты (GDPR).

В политике конфиденциальности теперь четко указано, что пользовательские данные TikTok передаются в ряд третьих стран для «важных функций», в том числе в Китай. Неясно, было ли это заявление сделано в связи с текущим расследованием GDPR, но новые условия могут лишить компанию возможности передавать данные пользователей из ЕС в соответствии с условиями, установленными решением Schrems II. TikTok заявил, что у него есть план локализации пользовательских данных из ЕС, но он не будет завершен как минимум до 2023 года.

Данные пользователей TikTok из ЕС отправлены в Китай и другие страны без соглашений об адекватности

Хотя материнская компания ByteDance ранее сталкивалась с проблемами при отправке пользовательских данных TikTok из США в Китай (после заверений, что она прекратит это делать), это обновление политики конфиденциальности применяется исключительно к странам Европы и должно вступить в силу 2 декабря.

Китай — лишь одна из ряда стран, с которыми пользовательские данные TikTok из ЕС и Великобритании передаются «сотрудникам корпоративной группы». В некоторых странах, таких как Канада, Израиль и Япония, действуют соглашения об адекватности данных. Другие, такие как Бразилия и Филиппины, этого не делают. В новой политике конфиденциальности также говорится, что данные пользователей TikTok из ЕС хранятся в США и Сингапуре; ни у одной из стран нет решения об адекватности, и опасения по поводу перехвата правительством США персональных данных ЕС - это то, что в первую очередь вызвало решение Шремса II.

TikTok заявляет, что у него есть юридически действительные стандартные договорные условия (SCC), которые охватывают передачу данных с этими разными

странами, но не сообщается, какие меры принимаются для защиты пользовательских данных от доступа извне.

Обновление политики конфиденциальности также не содержало подробностей о том, какие элементы пользовательских данных TikTok передаются этим иностранным сотрудникам, но в нем говорилось, что в некоторых случаях данные о местоположении передаются. Это может произойти, когда пользователи вручную добавляют местоположение к видео, которое они загружают, или когда они включают параметр «Службы определения местоположения для TikTok». Однако компания утверждает, что не собирает «точных» данных о местоположении, таких как GPS-координаты.

Юридические проблемы, связанные с международным перемещением пользовательских данных TikTok, вспыхнули в США в последний год правления администрации Трампа, когда она стремилась запретить компании доступ в магазины приложений из соображений национальной безопасности. Ирландский DPC проводит собственное расследование этой проблемы с 2021 года, но с упором на соблюдение GDPR в соответствии с условиями Schrems II, которые требуют, чтобы страны-партнеры имели сопоставимый закон о защите данных. Первоначальный проект решения по этому вопросу ожидается где-то в первом квартале 2023 года, а обязательные условия могут быть опубликованы в течение нескольких месяцев после этого.

Политика конфиденциальности вызывает вопросы о будущем статусе TikTok в Европе

Использование SCC не является гарантией законной передачи пользовательских данных TikTok в соответствии с условиями GDPR, поскольку каждый SCC должен оцениваться индивидуально, и неясно, были ли уже рассмотрены те, которые указаны в связи с политикой конфиденциальности.

Важным шагом TikTok для укрепления своего статуса в ЕС стало строительство центра обработки данных в Ирландии, которое ведется с 2020 года. Данные пользователей TikTok из ЕС будут храниться локально после завершения строительства объекта. Тем не менее, объект должен был быть завершен в начале 2022 года, но несколько раз переносился, последняя из которых перенесла ожидаемую дату открытия на 2023 год.

Скрытие пользовательских данных TikTok в США потенциально проливает некоторый свет на ситуацию, поскольку это произошло из-за утечки внутренних чатов компании, которые были переданы в СМИ. Содержание этих чатов в нескольких местах предполагает, что инженеры в Китае, по сути, имеют свободный доступ к пользовательским данным в США, и что филиалам TikTok в других странах часто необходимо предоставлять доступ китайскому персоналу, поскольку они просто не знают, как работают определенные аспекты платформы. Хотя это может показаться относительно безобидным внутренним делом, другие страны обеспокоены политикой национальной безопасности Китая, предоставляющей правительству свободный доступ к любым данным, хранящимся в стране.

TikTok, бесспорно, нанес серьезный ущерб связям с общественностью из-за того, что настаивал на поддержании связей с Китаем из других стран, но он также остается чрезвычайно популярным среди молодых пользователей (включая

несовершеннолетних пользователей, которые пользуются особой защитой в соответствии с национальным законодательством).

Клод Мэнди, главный евангелист по безопасности данных в Symmetry Systems, рассматривает это как курс на столкновение с жесткими правилами или даже запретами, если компания не начнет практиковать «радикальную» прозрачность, чтобы успокоить как родителей, так и членов правительства, которые обеспокоены национальной безопасностью: «Изменения TikTok в их политике конфиденциальности, чтобы отразить следует похвалить их реальную инженерную и мошенническую практику работы с учетными записями; хотя вызовет тревогу в первую очередь географическое распространение своих сотрудников с таким уровнем доступа. Многие родители, такие как я в Symmetry Systems, были бы рады видеть более постоянную и несколько радикальную прозрачность от технологических компаний, таких как TikTok, с подробным описанием количества сотрудников с таким уровнем доступа; и сколько информации от того, сколько пользователей TikTok было просмотрено в соответствии с различными законными способами использования, изложенными в политике». ***(Scott Ikeda. European TikTok User Data Found To Be Available To Chinese Staff as Company Updates Privacy Policy // CPO Magazine (https://www.cpomagazine.com/data-privacy/european-tiktok-user-data-found-to-be-available-to-chinese-staff-as-company-updates-privacy-policy/). 07.11.2022).***

***

«В течение некоторого времени среди потребителей уже наблюдался рост осведомленности о конфиденциальности, но скандал с Cambridge Analytica в 2018 году, похоже, стал тем инцидентом, который действительно сделал методы обработки данных общепринятыми. Растущее количество свидетельств свидетельствует о том, что средний человек теперь очень хорошо осведомлен о том, как компании отслеживают его поведение в Интернете, а новый отчет DataGrail указывает на то, что они перестанут вести дела с компаниями и услугами, которым они не доверяют.

Опрос потребительских настроений был проведен в июле, в нем приняли участие около 4000 респондентов из США и нескольких стран Европы. Результаты сравниваются с аналогичным опросом, проведенным в 2020 году, и растет обеспокоенность как личной конфиденциальностью, так и действиями, которые люди готовы предпринять для ее защиты. Поведение в Интернете также все больше зависит от доверия: потребители отказываются делиться своими данными с компаниями, которые не прозрачны в отношении того, как они обрабатываются, или которые были арестованы в прошлом за неправильное обращение с ними.

Осведомленность о конфиденциальности теперь чрезвычайно распространена, онлайн-потребители требуют уважения

Осведомленность о конфиденциальности более распространена, чем нет: 60% потребителей в настоящее время сообщают, что они обеспокоены своей конфиденциальностью в Интернете, а 53% считают, что они не контролируют свою онлайн-личность. 35% сказали, что им «надоело» использовать личные данные для показа целевой рекламы, а 25% говорят, что этот процесс им «жуткий».

В то время как потребители очень хорошо осведомлены о том, как компании отслеживают их поведение в Интернете на данный момент, 34% говорят, что они чувствуют себя «перегруженными», пытаясь управлять такими вещами, как настройки конфиденциальности и отказы от широкого спектра веб-сайтов и приложений, которые они используют. Хотя законодательство, такое как Общий регламент по защите данных (GDPR), было большим благом с точки зрения осведомленности о конфиденциальности, оно также создало такие проблемы, как «усталость от файлов cookie». Обязательные баннеры, которые предлагают пользователям веб-сайтов настроить свои параметры файлов cookie, полезны, но их появление на каждом веб-сайте побудило некоторых конечных пользователей просто пропустить их как можно быстрее, учитывая совокупное время, которое занимает процесс.

Осведомленность о конфиденциальности, по-видимому, наиболее актуальна в отношении продажи персональных данных третьим лицам. 75% теперь говорят, что им известно о компаниях, с которыми они ведут бизнес, продавая личную информацию третьим лицам, по сравнению с 62% в опросе 2020 года. 85% говорят, что хотели бы точно знать, какие компании отслеживают онлайн-поведение и как используются собираемые ими данные, а 79% хотят иметь контроль над тем, как компании могут использовать собираемые ими данные.

Конкретные действия, предпринимаемые для защиты личных данных, становятся все более популярными вместе с этим всплеском осведомленности о конфиденциальности. Чуть больше половины респондентов теперь говорят, что они продолжают удалять файлы cookie и историю браузера, а также отказываются от подписки на нежелательные электронные письма. Примерно каждый третий использует блокировщик рекламы, управляет своими маркетинговыми предпочтениями для сайтов и приложений, которые они используют, а также использует режимы «инкогнито» ОС и браузера. Чуть менее трети используют менеджеры паролей и функции «не отслеживать» (например, настройки, которые теперь встроены в iOS от Apple), и чуть менее четверти используют многофакторную аутентификацию для безопасного входа в систему.

Когда-то было широко распространено мнение, что люди были бы счастливы отдать личную информацию в обмен на «бесплатные» услуги, но эта модель все чаще зависела от общего отсутствия осведомленности о конфиденциальности. Чем больше люди узнают, как отслеживается их онлайн-поведение, тем больше они готовы платить за конфиденциальность. 67% респондентов заявили, что будут платить до 100 долларов в год за защиту своей конфиденциальности, а 2% заявили, что готовы платить до 5000 долларов в год.

Хотя эти 2%, готовые платить часть своей годовой зарплаты за защиту своей конфиденциальности, могут быть исключением, существует общая тенденция, когда покупатели с более высокими доходами доверяют свой бизнес брендам, которым они доверяют свои личные данные. Около трех из четырех респондентов заявили, что перестанут делать покупки у любимого ритейлера, если узнают, что их личные данные не в безопасности, а также заявили, что готовы заплатить «на несколько долларов больше», чтобы делать покупки у бренда, который им нравится. можно доверять. А 80% заявили, что прозрачность в отношении обработки персональных

данных и отслеживания поведения в Интернете является фактором их лояльности к бренду.

Конфиденциальность — это желание двух партий, но поведение в Интернете может измениться из-за политических событий.

Осведомленность о конфиденциальности и стремление к надежной защите данных преодолевают все политические разногласия, но конкретные политические события могут привести к изменениям в поведении в Интернете. В ходе исследования DataGrail респондентов из США спросили, как отмена дела Роу против Уэйда повлияла на их осведомленность о конфиденциальности и способы использования ими онлайн-сервисов. 66% женщин поколения Z и миллениалов заявили, что планируют изменить или удалить приложения для отслеживания менструального цикла с момента принятия решения, и половина уже сделала это. Также после изменения закона увеличилось использование режима инкогнито в браузерах, отказ от обмена данными с правительством, удаление данных, очистка онлайн-профилей и использование поддельных профилей и документации.

Независимо от политических взглядов, более половины всех респондентов также говорят, что они считают неприкосновенность частной жизни одним из прав человека и должны быть подкреплены защитой федерального законодательства.

Респонденты также выразили свои самые большие опасения по поводу конфиденциальности и больше всего обеспокоены тем, что их электронная почта может быть взломана. Также в списке находятся чрезмерный сбор данных для личных профилей компаниями, утечка данных, неправильное обращение со стороны правительства (или сторонних подрядчиков) и продажа личной информации брокерам данных.

Основываясь на собранной информации, рекомендации отчета включают повышение прозрачности методов обработки данных, уважение предпочтений потребителей (в частности, отказ от отправки им электронных писем с разных адресов после того, как они отказались от подписки), а также разработку политики конфиденциальности и методов осуществления прав на конфиденциальность». ***(Scott Ikeda. Study Shows Privacy Awareness Is the “New Normal” for Consumers, Online Behavior Is Much More Guarded // CPO Magazine (https://www.cpomagazine.com/data-privacy/study-shows-privacy-awareness-is-the-new-normal-for-consumers-online-behavior-is-much-more-guarded/). 04.11.2022).***

***

«В новом отчете The Intercept раскрываются ранее неизвестные подробности об иранской системе SIAM, которая имеет базовый доступ к сотовым сетям страны. Система используется не только для правительственной слежки, но также имеет функции, позволяющие удаленно манипулировать отдельными коллекциями данных и бэкдорами посредством шифрования.

Считается, что система использовалась для мониторинга и отслеживания протестующих в последние месяцы, и ее функции позволяют отключать отдельных пользователей от сетей 3G или 4G и заставлять их использовать более медленное соединение 2G. В некоторых случаях местная полиция также отправляла текстовые

сообщения определенным пользователям, предупреждая их держаться подальше от зон протеста и не связываться с «антиреволюционными» критиками правительства.

Правительство Ирана внедрило слежку за телефонными сетями страны

Нынешняя волна протестов в Иране была вызвана сентябрьской смертью Махсы Амини во время содержания под стражей в полиции по делам нравов, молодой женщины, которую задержали за то, что она не носила чадру на публике, как того требует строгий дресс-код страны. С тех пор протестное движение превратилось в общую оппозицию теократическому правительству страны. Протестующие жаловались на спорадические отключения сети, медленные соединения и сбои в работе приложений с тех пор, как это началось, и в отчете о перехвате приводятся доказательства того, что это происходит из-за прямого наблюдения и вмешательства со стороны правительства.

Информация о системе SIAM получена из просочившихся документов, полученных от иранского оператора сотовой связи Ariantel, которые содержат переписку по электронной почте и документы, которыми обмениваются сотрудники и иранское правительство, а также внешние подрядчики, используемые для внедрения и обслуживания системы. В архиве также есть два руководства для операторов, в которых описаны функции, разработанные специально для правительственной слежки и вмешательства в сообщения критиков правительства.

Протестующие и правительственные диссиденты уже давно подозревают широкомасштабную слежку со стороны правительства через телефонные сети страны, но до сих пор подробности не были известны. SIAM позволяет правительственным агентам подключаться к веб-интерфейсу, который предоставляет подробные данные о пользователях мобильных телефонов, а также меню действий, которые могут быть предприняты против них: инструменты для взлома шифрования, сводки метаданных для определенных телефонных номеров, которые показывают полные записи их сетей. связь и возможность замедлять их соединения, блокируя телефоны в сетях выше 3G, чтобы принудительно установить резервное соединение 2G.

Таким образом, система выходит за рамки государственного надзора и служит инструментом активного противодействия и срыва протестов. Агентством, ответственным за это, является Регуляторный орган связи (CRA), ведущий регулятор телекоммуникаций страны. Одним из документов, полученных The Intercept, является меморандум, уведомляющий всех операторов связи о том, что они должны предоставить агентству прямой доступ к своим системам для «запроса информации о клиенте» и «изменения (клиентских) услуг через веб-сервис».

Управление безопасности коммуникационных систем (OSCS), которое является частью CRA, по-видимому, является организацией, наиболее непосредственно связанной с правительственным наблюдением и нарушением обслуживания через SIAM. Просочившиеся документы показывают, что обмен электронной почтой между оператором связи Ariantel и OSCS датируется не позднее августа этого года, а руководство по эксплуатации SIAM также, по-видимому, было переведено на английский язык и предоставлено испанскому телекоммуникационному подрядчику, с которым Ariantel вела дела.

Меню функций отслеживает номера IMEI устройств, подталкивает цели к сетям 2G.

Помимо правительственного надзора, большая часть внимания SIAM, по-видимому, направлена на продвижение выбранных целей в сети 2G. Помимо снижения скорости (до такой степени, что многие функции смартфона становятся практически бесполезными), это также снижает безопасность его связи, поскольку сети 2G не предлагают такие же функции шифрования. Эта функция «Force2GNumber» в SIAM может быть развернута как средство, облегчающее перехват кодов двухфакторной аутентификации в SMS, что может обеспечить маршрут к зашифрованным приложениям для обмена сообщениями, обычно используемым протестующими.

SIAM также может отслеживать общение между пользователями сети по номеру IMEI устройства. Это означает, что протестующие могут постоянно отслеживаться, даже если они меняют SIM-карты, а их общение и передвижения могут быть связаны с различными данными, которые SIAM может получать непосредственно от оператора связи: фамилия, национальность, история местоположений, контактная информация для выставления счетов, дата рождения. номер сертификата (часто используется в качестве национального идентификационного номера), работодатель и список IP-адресов и сетей Wi-Fi, к которым подключался пользователь.

Хотя CRA якобы является регулирующим органом, давно известно, что он играет активную роль в цензуре интернет-коммуникаций в Иране. Агентство попало под санкции США в 2013 году за блокировку сотен веб-сайтов во время споров 2009 года о результатах президентских выборов в Иране. А в 2019 году было обнаружено, что CRA напрямую приказало некоторым интернет-провайдерам закрыться во время очередного периода социальных волнений.

В документах не прослеживается прямая связь между правительственным надзором за протестующими и использованием SIAM, но руководство по функциям, по-видимому, специально разработано для отслеживания и подавления инакомыслия. И он отслеживает общие отчеты протестующих на местах в Иране, которые говорят, что обслуживание часто замедляется или останавливается во время протестов и что они получают неожиданные сообщения от правительственных учреждений, которые внезапно советуют им избегать районов запланированных акций протеста». ***(Scott Ikeda. Embedded in Cellular Networks, Iran's SIAM System Allows for Remote Phone Manipulation // CPO Magazine (https://www.cpomagazine.com/data-privacy/embedded-in-cellular-networks-irans-siam-system-allows-for-remote-phone-manipulation/). 02.11.2022).***

***

«Любой, кто совершил онлайн-покупку в See Tickets в последние годы, может стать жертвой кражи кредитной карты, поскольку компания сообщила, что с июня 2019 года по январь 2022 года на ее веб-сайте работал скиммер.

See Tickets принадлежит крупному развлекательному конгломерату Vivendi и работает в США, Канаде и многих странах Европы. В последние годы компания

продавала до 20 миллионов билетов в год, обслуживая крупные мероприятия, такие как фестиваль в Гластонбери, LA Pride и музыкальный фестиваль Pitchfork.

Кража кредитной карты оставалась незамеченной в течение многих лет, на полное исправление ушло девять месяцев

See Tickets запустила новую цифровую систему продажи билетов в 2019 году, предназначенную для борьбы с автоматическими ботами, которые скупают билеты и «скальпируют» их по завышенным ценам, добавляя штрих-код, привязанный к личному онлайн-профилю. Но за несколько месяцев до того, как эта система заработала, хакеры незаметно проникли в компанию и разместили на неизвестном домене скиммер, предназначенный для кражи кредитных карт.

Остается неясным, какие именно регионы мира пострадали и сколько всего жертв кражи кредитных карт, поскольку See Tickets не опубликовала много информации об атаке. У компании есть глобальный веб-сайт в дополнение к пяти региональным доменам, и до сих пор неизвестно, какой из них был затронут.

Известно, что скиммер был разработан для перекачки всей платежной информации, введенной в процессе онлайн-покупки: полное имя, платежный адрес с почтовым индексом, номер карты, код CVV и срок действия. В компании уточнили, что банковская информация, номера социального страхования и государственные идентификационные номера не были украдены (в тех случаях, когда они могли быть запрошены при покупке).

Скиммер состоял из кода JavaScript, вставленного на страницу покупки во время взлома 25 июня 2019 года. Компания обнаружила нарушение в апреле 2021 года, но не могла полностью удалить вредоносный код до января 2022 года. Согласно внутреннему расследованию, завершившемуся в сентябре этого года окно кражи кредитных карт, возможно, было открыто в течение всего этого периода чуть более 30 месяцев.

Публичное уведомление, недавно опубликованное See Tickets, призывает клиентов проявлять бдительность в отношении несанкционированных покупок, появляющихся на любых картах, которые они могли использовать для покупки билетов, но не предлагает никакой помощи или новой контактной информации для тех, кто считает, что они могли быть жертвами. кража кредитной карты.

Пока нет информации от See Tickets о географическом диапазоне, но считается, что это коснется клиентов в нескольких штатах США.

Хотя See Tickets не подтвердила, какие именно страны были затронуты (или была ли взломана вся глобальная система), есть некоторые крохи информации, указывающие на то, что клиенты из США были затронуты как минимум.

Информация о краже кредитной карты взята из уведомления об утечке данных, поданного в Генеральную прокуратуру Монтаны, но в нем также указана контактная информация для ресурсов по краже личных данных для ряда других штатов.

Аналогичное уведомление было направлено Генеральному прокурору Техаса, в котором указывалось, что около 92 000 клиентов See Tickets в штате пострадали от кражи кредитных карт, связанной с инцидентом. Сообщается, что письма с уведомлением о взломе были отправлены каждой из этих жертв 24 октября.

Использование электронных скиммеров для кражи кредитных карт в Интернете резко возросло с началом пандемии Covid-19 и продолжает оставаться на

повышенном уровне. Это было озаглавлено атаками Magecart, особая вредоносная программа, используемая несколькими известными киберпреступными группировками. Magecart и подобные продвинутые скиммеры часто задерживаются на сайтах-жертвах месяцами (или годами в данном случае), потому что автоматические поисковые роботы и сканеры часто не могут их обнаружить. Вредоносный код часто скрывается путем внедрения скриптов, вызывающих его с удаленного сервера, на страницу, а не непосредственного размещения на целевом веб-сайте. Группы опытных скиммеров также используют новое доменное имя для каждой из этих новых атак, чтобы еще больше скрыться от автоматизированных систем обнаружения, и обычно объединяют вредоносный код с законными средами JavaScript, чтобы сделать его менее заметным.

Онлайн-скиммеры также представляют собой особую проблему кражи кредитных карт, поскольку конечный пользователь мало что может сделать, чтобы защитить себя. Домашние антивирусные и антивредоносные системы обычно не замечают скиммеры во время совершения онлайн-покупки, и атака никоим образом не изменяет внешний вид или функции законных сайтов. По сути, клиенты должны полагаться на сайт электронной коммерции, чтобы обеспечить их внутреннюю безопасность, но можно добавить дополнительный уровень защиты, используя промежуточные платежные системы, которые требуют отдельного входа во время оплаты (например, PayPal), когда опция доступна.

Как отмечает Эрих Крон, специалист по вопросам безопасности в KnowBe4, компании, принимающие онлайн-платежи, должны включать регулярные проверки кода в свои меры безопасности, чтобы гарантировать, что их невольно не используют в качестве фермы для кражи кредитных карт: «Это было очень долгое время, чтобы код, подобный этому, работает на веб-сайте организации. Кроме того, время, прошедшее с момента его обнаружения до момента его удаления, было исключительно долгим. Проверка кода является необходимой частью работы веб-сайта электронной коммерции с любым значительным объемом трафика. Должны быть разработаны планы реагирования на инциденты, чтобы быстро справляться с экземплярами вредоносного ПО либо внутри организации, либо на веб-сайте». ***(Scott Ikeda. Over Two Years of Credit Card Theft: See Tickets Discloses Online Skimmer That Has Been Operating Since Mid-2019 // CPO Magazine (https://www.cpomagazine.com/cyber-security/over-two-years-of-credit-card-theft-see-tickets-discloses-online-skimmer-that-has-been-operating-since-mid-2019/). 02.11.2022).***

***

«Thomson Reuters признал утечку базы данных, в результате которой было раскрыто не менее 3 ТБ данных о клиентах, хотя многонациональный медиа-конгломерат попытался преуменьшить серьезность проблемы.

По данным исследовательской группы Cybernews, Thomson Reuters оставил три базы данных незащищенными, чтобы любой мог получить к ним доступ без аутентификации. Сайт информационных новостей сообщил, что одна из баз данных содержала «конфиденциальную актуальную информацию со всех платформ компании».

Эксперты по безопасности предупредили, что злоумышленники используют данные для выполнения атак, начиная от социальной инженерии и заканчивая программами-вымогателями.

Утечка базы данных Thomson Reuters раскрыла конфиденциальную платформу и данные клиентов

Согласно Cybernews, одна утечка базы данных содержала «конфиденциальные данные о клиентах и корпорации, включая пароли сторонних серверов в текстовом формате».

База данных ElasticSearch содержала 6,9 миллиона уникальных журналов, собранных при взаимодействии с клиентами, включая журналы входа в систему и сброса пароля. Хотя они не раскрывают пароли пользователей, журналы показывают адрес электронной почты владельца учетной записи и время, когда они инициировали запрос на смену пароля.

Кроме того, в журналах отображался запрос SQL (язык структурированных запросов) о том, что искали клиенты Thomson Reuters, и полученные ими результаты, включая корпоративную и юридическую информацию.

Утечка также раскрыла корпоративную и юридическую информацию для юридических и физических лиц. Например, продукт компании ONESOURCE Global Trade позволяет клиентам искать информацию об экспортно-импортном контроле, ограничениях и санкциях. По данным исследователей, сотрудник американской компании провел поиск в российской компании с помощью инструмента Thomson Reuters и обнаружил, что члены правления находятся под санкциями США.

По данным Cybernews, открытый экземпляр был проиндексирован популярными поисковыми системами IoT, что расширило поверхность атаки. Cybernews не смог определить или не сообщил, имел ли кто-либо из злоумышленников доступ к раскрытым данным клиентов. Однако киберпреступники обычно обнаруживают открытые облачные базы данных в течение нескольких минут.

Thomson Reuters преуменьшает утечку базы данных

Thomson Reuters пояснил, что «отдельная ошибка в среде продукта привела к непреднамеренной неправильной настройке непроизводственной среды».

Медиа-гигант пояснил, что две открытые базы данных должны были быть общедоступными. Компания заявила, что третья база данных была «непроизводственным сервером», содержащим журналы приложений из предпроизводственной среды, и была доступна только «небольшой части клиентов Thomson Reuters Global Trade».

Медиа-гигант оправдывал механизм логирования тем, что «сервер содержит информацию, необходимую для оперативной поддержки платформы».

Cybernews пояснил, что, хотя нерабочий сервер может не хранить данные приложения, такая информация не менее конфиденциальна.

Тем не менее, медиакомпания защитила базу данных, начала расследование и начала уведомлять клиентов.

Cybernews предположил, что утечка базы данных произошла из-за «неправильной настройки сервиса AWS Elastic Load Balancing» с различными правилами, которые не полностью охватывают элементы управления доступом.

«Независимо от того, насколько крупной или надежной является компания, они представляют собой одну неправильную конфигурацию от взлома», — сказал Дэвид Мейнор, старший директор по анализу угроз в Cybrary. «Подобные проблемы — вот почему вам нужно инвестировать не только в инструменты. Инвестиции в масштабирование вашего персонала важны как никогда».

Утечка базы данных Thomson Reuters создала серьезную угрозу безопасности

Cybernews предположили, что раскрытие конфиденциальных данных, таких как информация о проверке отдельных лиц или организаций, может предупредить организации, занимающиеся тайными теневыми сделками.

Кроме того, неправильная конфигурация базы данных глобальных торговых клиентов Thomson Reuters может спровоцировать атаку на цепочку поставок, раскрывая критически важную системную информацию.

«Раскрытие строк подключения особенно опасно, потому что открыты элементы внутренней сети компании, что позволяет злоумышленникам перемещаться по горизонтали и перемещаться по внутренним системам Reuter Thomson», — пишут исследователи.

Мантас Саснаускас, руководитель отдела исследований в области безопасности Cybernews, предупредил, что утечка базы данных может также позволить злоумышленникам закрепиться в системах, используемых партнерами Thomson Reuters.

Злоумышленники также могут продавать учетные данные для входа, такие как пароли серверов, брокерам начального доступа или группам программ-вымогателей для выполнения изощренных атак. Утечка данных клиентов подвергла их атакам социальной инженерии, таким как поддельные счета и счета с вредоносным ПО от злоумышленников, выдающих себя за Thomson Reuters.

«Сегодняшний взлом Thomson Reuters звучит как вопиющая ошибка и, вероятно, будет иметь серьезные каскадные последствия для корпоративного управления, процессов и надзора», — сказал Раджив Пимпласкар, генеральный директор Dispersive Holdings. «Поскольку Thomson Reuters является важным поставщиком для многих компаний из списка Fortune 500, этот инцидент также может иметь последствия для третьих сторон и цепочки поставок для их клиентов и деловых партнеров».

Утечка базы данных Thomson Reuters может раскрыть больше данных о клиентах, чем ожидалось

Исследователи предсказали, что открытая база данных содержит более конфиденциальные данные о клиентах, которые они не могут обнаружить, не нарушая законных границ.

Тем не менее исследователи указали, что база данных оставалась открытой менее недели.

Ограниченный анализ утечки базы данных показывает, что часть данных о клиентах была утекла совсем недавно, 26 октября, в то время как база данных оставалась открытой с 21 октября.

Исследователи пояснили, что поисковые системы не возвращали никаких утекших данных за пределами этого окна, предполагая, что ранее база данных не была общедоступной.

Thomson Reuters утверждает, что его политика конфигурации соответствует лучшим практикам безопасности. Кроме того, медиа-конгломерат заявил, что он выполняет автоматизированное и централизованное ведение журналов для предоставления предупреждений в режиме реального времени.

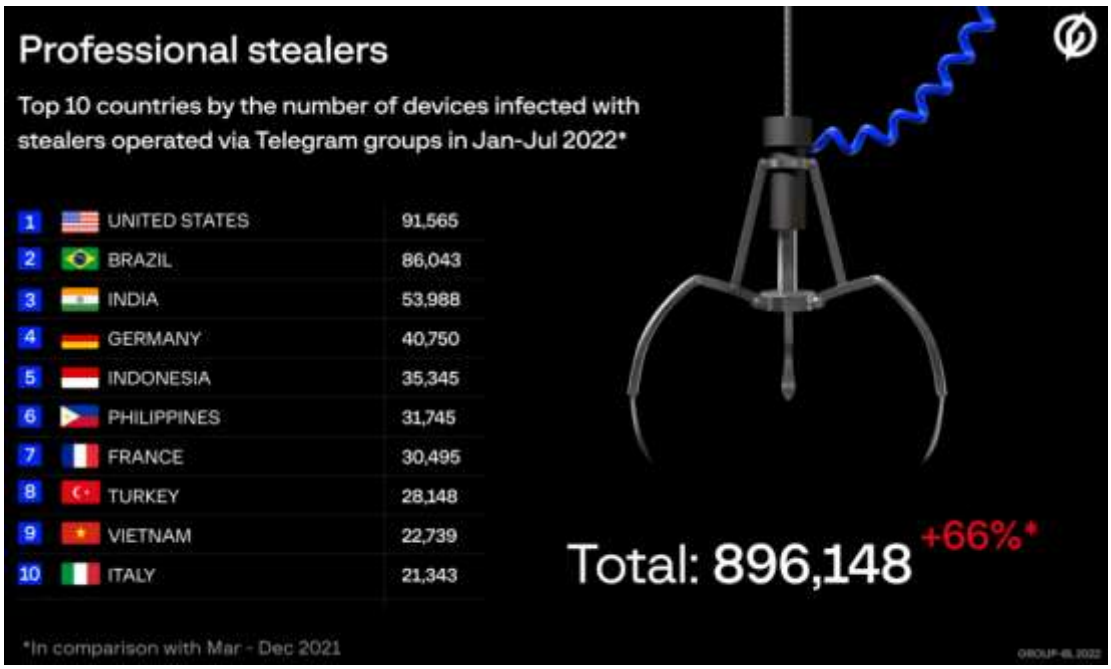
«Между тем данные показывают, что инстанс был открыт более трех дней подряд. Напрашивается вопрос, нужны ли оповещения в режиме реального времени, если некому просматривать оповещения», — сказал Мартинас Варейкис, исследователь информационной безопасности Cybernews». ***(Alicia Hope. Thomson Reuters Database Leak Exposed 3TB of Sensitive Platform and Customer Data // CPO Magazine (https://www.cpomagazine.com/cyber-security/thomson-reuters-database-leak-exposed-3tb-of-sensitive-platform-and-customer-data/). 01.11.2022).***

***

«По меньшей мере 34 отдельные русскоязычные группы киберпреступников, использующие вредоносные программы для кражи информации, такие как Raccoon и Redline, в совокупности украли 50 350 000 паролей к учетным записям из более чем 896 000 отдельных заражений с января по июль 2022 года.

Украденные учетные данные предназначались для криптовалютных кошельков, учетных записей Steam, Roblox, Amazon и PayPal, а также записей платежных карт.

Согласно отчету Group-IB, чьи аналитики отслеживают эти операции по всему миру, большинство жертв базируются в США, Германии, Индии, Бразилии и Индонезии, но вредоносные операции были нацелены на 111 стран.



Страны с наибольшим количеством случаев заражения в период с января по июль 2022 г. (Группа IB)

Восстание инфокрадов

В 2022 году распространение вредоносного ПО для кражи информации достигло беспрецедентного уровня, и теперь в нем участвуют низкоквалифицированные хакеры, стремящиеся получить большую прибыль от своей незаконной деятельности.

Group-IB заявляет, что киберпреступники, способствующие росту распространения программ для кражи информации, — это мошенники низкого уровня, которые ранее работали как «звонящие жертвы» в фишинговых кампаниях, известных как «Classiscam».

«Приток огромного числа работников в популярную аферу Classiscam [...] на пике популярности, состоящую из более чем тысячи преступных групп и сотен тысяч поддельных веб-сайтов, привел к тому, что преступники конкурируют за ресурсы и ищут новые способы получать прибыль», — комментирует Group-IB.

«Популярность схем с участием стиллеров объясняется низким порогом входа. Новичкам не нужно обладать продвинутыми техническими знаниями, так как процесс полностью автоматизирован, а единственная задача работника — создать файл со стилером в боте Telegram и привлечь к нему трафик». - Группа-ИБ

В настоящее время в Telegram существует 34 активные группы киберпреступников, которые действуют как массовые банды по краже информации, каждая из которых насчитывает около 200 членов.

23 группы используют стилер Redline, восемь используют Raccoon, а три используют собственное вредоносное ПО.

SEKOIA также отметила ранее на этой неделе, что еще один похититель информации под названием «Аврора» набирает обороты на подпольных форумах и уже принят на вооружение семью известными группами угроз.

Увеличение активности по краже информации показано в статистике, составленной отчетом Group-IB, который сравнил 10-месячный период в 2021 году с семимесячным периодом в 2022 году.

Украдено паролей: 50 352 518 (рост на 80%).

Удалено файлов cookie: 2 117 626 523 (рост на 74%).

Взлом криптокошельков: 113 204 (рост на 216%).

Скомпрометировано платежных карт: 103 150 (рост на 81%).

Статистика работы Infostealer за первые семь месяцев 2022 года (Group-IB)

Group-IB также отмечает, что в первые семь месяцев этого года актеры сосредоточились на краже учетных записей Steam, Epic Games и Roblox, зафиксировав пятикратный рост по сравнению с прошлым годом.

Операции на основе Telegram

Telegram играет жизненно важную роль в деятельности этих кибербанд, как в организации их кампаний, так и в поддержании функциональной структуры, позволяющей им осуществлять кражу данных.

Эти частные каналы Telegram предлагают оперативникам поддержку и техническое руководство, могут служить точками утечки данных, размещать важные объявления, выступать в качестве порталов для сообщений об ошибках, а также содержат ботов, которые могут создавать пользовательские сборки вредоносных программ для клиентов 24/7.

Группы по-прежнему соблюдают иерархические правила, при этом «администраторы», занимающие верхние строчки, продают доступ к вредоносным программам для кражи информации «рабочим» за несколько сотен долларов в месяц.

Рабочие несут ответственность за привлечение трафика на сайты с вредоносным ПО, что они делают с помощью видео на YouTube, BlackSEO, отравления SEO, загруженных торрент-файлов или вредоносных сообщений в социальных сетях.

Пользователи могут свести к минимуму вероятность заражения программами для кражи информации, избегая загрузок из сомнительных источников, проверяя все загружаемые исполняемые файлы с помощью антивирусного решения перед открытием и поддерживая свою систему в актуальном состоянии». ***(Bill Toulas. Russian cybergangs stole over 50 million passwords this year // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/russian-cybergangs-stole-over-50-million-passwords-this-year/). 23.11.2022).***

***

«Ирландская комиссия по защите данных (DPC) оштрафовала Meta на 265 миллионов евро (275,5 миллиона долларов) за массовую утечку данных Facebook в 2021 году, в результате которой была раскрыта информация сотен миллионов пользователей по всему миру.

На этом заканчивается расследование DPC потенциальных нарушений GDPR со стороны Meta, начатое 14 апреля 2021 года после публикации на хакерском форуме данных, принадлежащих 533 миллионам пользователей Facebook.

Выставленные данные включали личную информацию, такую как номера мобильных телефонов, идентификаторы Facebook, имена, пол, местоположение, статусы отношений, занятия, даты рождения и адреса электронной почты.

Все эти данные были размещены на известном хакерском форуме, что позволило злоумышленникам использовать эти данные для целенаправленных атак.

Facebook в то время заявил, что злоумышленники собирали данные, используя уязвимость в своем инструменте «Импорт контактов», чтобы связать номера телефонов с идентификатором Facebook, а затем соскребая остальную информацию для создания профиля пользователя.

Платформа заявила, что исправила ошибку в 2019 году, а данные были собраны до этого.

Расследование DPC пришло к выводу, что Meta (тогда Facebook) нарушила статьи 25 (1) и 25 (2) GDPR, которые резюмируются следующим образом:

25 (1) - Контроллер данных должен применять соответствующие технические и организационные меры, такие как псевдонимизация, и интегрировать необходимые меры безопасности в обработку для выполнения требований настоящего Регламента и защиты прав субъектов данных.

25 (2) - Контролер должен принять соответствующие технические и организационные меры для обеспечения того, чтобы по умолчанию обрабатывались только персональные данные, необходимые для каждой цели обработки. В частности, такие меры должны гарантировать, что по умолчанию персональные данные не станут доступными без вмешательства физического лица для неопределенного числа физических лиц.

«Был проведен всеобъемлющий процесс расследования, включая сотрудничество со всеми другими надзорными органами по защите данных в ЕС», — говорится в сообщении DPC.

«Эти надзорные органы согласились с решением КДС».

Скрапинг данных

Скребки данных — это автоматизированные боты, которые используют открытые сетевые API-интерфейсы платформ, хранящих пользовательские данные, таких как Facebook, для извлечения общедоступной информации и создания массивных баз данных профилей пользователей.

Несмотря на отсутствие взлома, наборы данных, собранные скребками, могут быть объединены с данными из нескольких точек (сайтов), создавая полные профили пользователей, что делает их отслеживание со стороны маркетологов или нацеливание со стороны злоумышленников намного более эффективным.

Однако в случае с Meta злоумышленники использовали уязвимость в Contact Importer в Facebook и Instagram, чтобы связать номера телефонов с этой общедоступной информацией, что позволило им создавать профили, содержащие личную и общедоступную информацию.

Парсинг противоречит политике большинства онлайн-платформ, но соблюдение этих правил технически сложно, как это недавно было подчеркнуто TikTok и WeChat.

LinkedIn подала в суд, чтобы предотвратить очистку данных на платформе, обеспечив судебный запрет против законных операторов скрейпинга и запретив им использовать данные, которые они уже собрали таким образом.

DPC считается авангардом соблюдения GDPR в ЕС из-за того, что многие технологические компании работают из Ирландии, поэтому его решение обязательно создаст турбулентность для других контроллеров больших данных, заставив их переоценить свои механизмы защиты от скрейпинга». ***(Bill Toulas. Meta fined €265M for not protecting Facebook users' data from scrapers // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/meta-fined-265m-for-not-protecting-facebook-users-data-from-scrapers/). 28.11.2022).***

***

«Более 5,4 миллиона пользовательских записей Twitter, содержащих непубличную информацию, украденную с помощью уязвимости API, исправленной в январе, были бесплатно размещены на хакерском форуме.

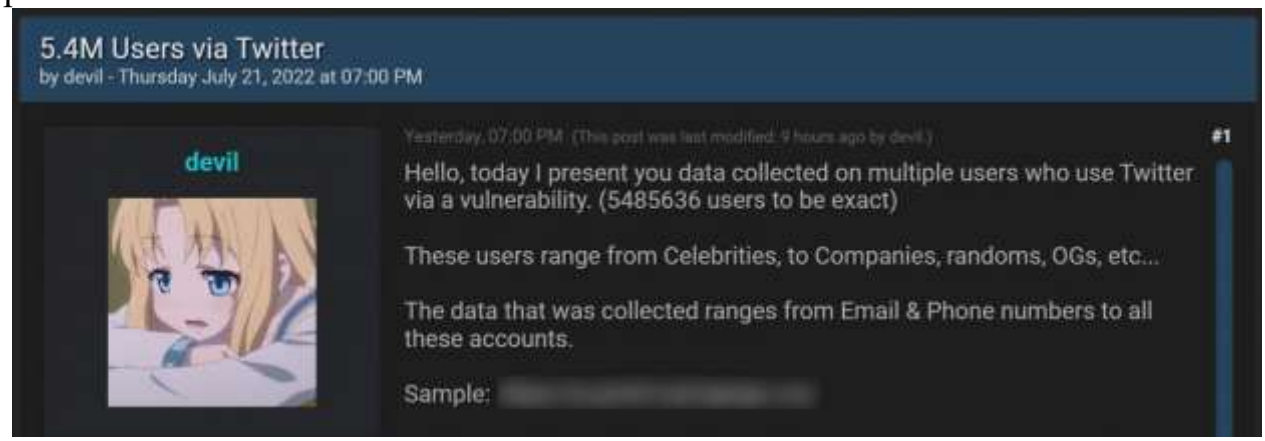
Еще один массивный, потенциально более значительный сброс данных миллионов записей Twitter также был раскрыт исследователем безопасности, демонстрируя, насколько широко злоумышленники злоупотребляли этой ошибкой.

Данные состоят из извлеченной общедоступной информации, а также частных номеров телефонов и адресов электронной почты, которые не предназначены для публичного доступа.

Нарушение данных Twitter

В июле прошлого года злоумышленник начал продавать личную информацию более 5,4 миллиона пользователей Twitter на хакерском форуме за 30 000 долларов.

Хотя большая часть данных состояла из общедоступной информации, такой как идентификаторы Twitter, имена, логины, местоположения и проверенный статус, они также включали личную информацию, такую как номера телефонов и адреса электронной почты.



Сообщение на форуме о продаже очищенных данных Twitter

Источник: BleepingComputer

Эти данные были собраны в декабре 2021 года с использованием уязвимости Twitter API, раскрытой в программе вознаграждения за обнаружение ошибок HackerOne, которая позволяла людям отправлять номера телефонов и адреса электронной почты в API для получения связанного идентификатора Twitter.

Используя этот идентификатор, злоумышленники могут затем очистить общедоступную информацию об учетной записи, чтобы создать запись пользователя, содержащую как личную, так и общедоступную информацию, как показано ниже.

Отредактированный пример одной из просочившихся записей пользователя Twitter

Источник: BleepingComputer

Неясно, была ли раскрыта информация о HackerOne, но BleepingComputer сообщили, что несколько злоумышленников использовали ошибку для кражи личной информации из Twitter.

После того, как BleepingComputer поделился образцом пользовательских записей с Twitter, социальная сеть подтвердила, что они пострадали от утечки данных из- за ошибки API, исправленной в январе 2022 года.

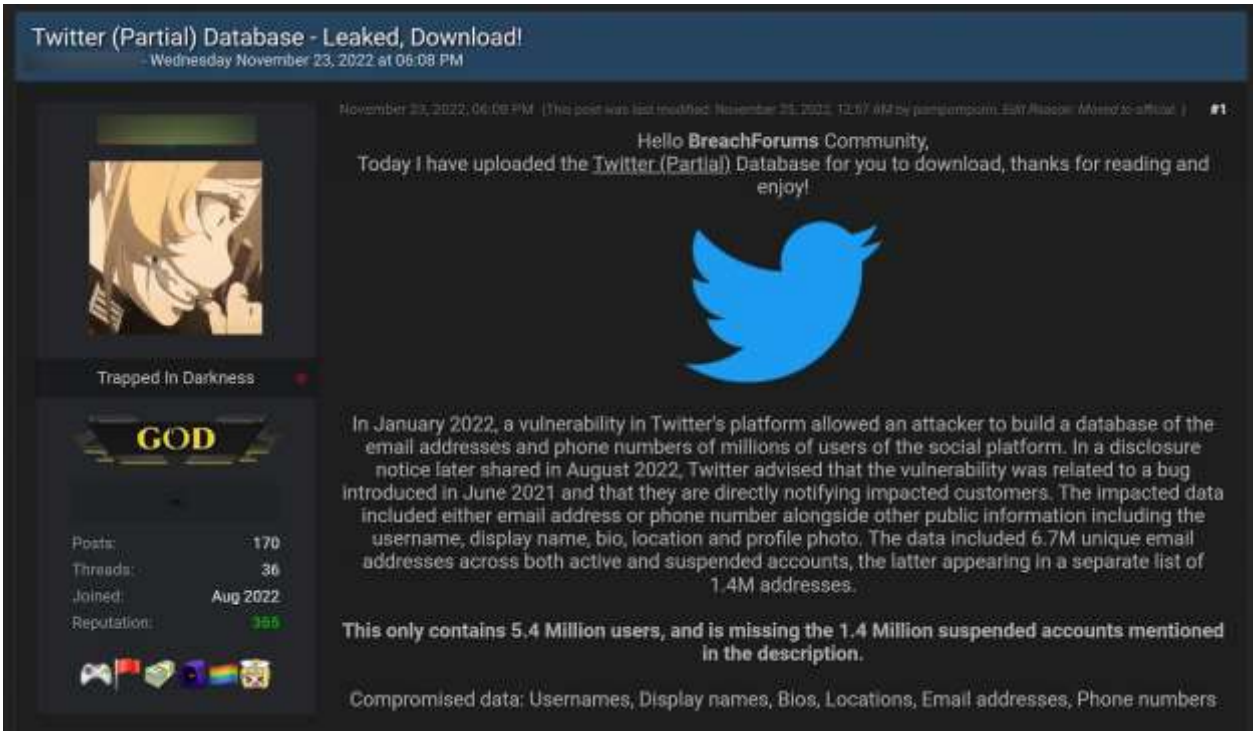
Помпомпурин, владелец хакерского форума Breached, сообщил BleepingComputer в эти выходные, что они несут ответственность за использование ошибки и создание массивного дампа записей пользователей Twitter после того, как другой злоумышленник, известный как «Дьявол», поделился с ними уязвимостью.

В дополнение к 5,4 миллионам записей для продажи были также дополнительные 1,4 миллиона профилей Twitter для заблокированных пользователей, собранных с использованием другого API, в результате чего общее количество профилей Twitter, содержащих личную информацию, достигло почти 7 миллионов.

Помпомпурин сказал, что этот второй дамп данных не был продан, а был передан только в частном порядке нескольким людям.

Данные Twitter поделились на хакерском форуме

В сентябре, а теперь совсем недавно, 24 ноября, 5,4 миллиона записей в Твиттере были бесплатно размещены на хакерском форуме.



5,4 миллиона записей в Твиттере утекли в сеть бесплатно
Источник: BleepingComputer

Помпомпурин подтвердил BleepingComputer, что это те же данные, которые были выставлены на продажу в августе, и включают 5 485 635 записей пользователей Twitter.

Эти записи содержат либо частный адрес электронной почты, либо номер телефона, а также общедоступные очищенные данные, включая идентификатор учетной записи в Твиттере, имя, отображаемое имя, проверенный статус, местоположение, URL-адрес, описание, количество подписчиков, дату создания учетной записи, количество друзей, количество избранных, количество статусов и URL-адреса изображения профиля.

Еще больший дамп данных, созданный в частном порядке

Хотя настораживает тот факт, что 5,4 миллиона записей были опубликованы злоумышленниками бесплатно, предполагается, что с помощью той же уязвимости был создан еще больший дамп данных.

Этот дамп данных потенциально может содержать десятки миллионов записей Twitter, состоящих из личных номеров телефонов, собранных с помощью той же ошибки API, и общедоступной информации, включая подтвержденный статус, имена учетных записей, идентификатор Twitter, биографию и отображаемое имя.

Новость об этой более серьезной утечке данных поступила от эксперта по безопасности Чада Лодера, который первым сообщил новость в Твиттере и вскоре после публикации был отстранен от работы. Впоследствии Лодер опубликовал отредактированный образец этой крупной утечки данных на Mastodon.

«Я только что получил доказательства массовой утечки данных Twitter, затронувшей миллионы учетных записей Twitter в ЕС и США. Я связался с несколькими затронутыми учетными записями, и они подтвердили, что взломанные данные верны. Это нарушение произошло не ранее 2021 года», Лодер поделился в Twitter.

Чад Лодер делится новостями о более крупном взломе Mastodon
Источник: BleepingComputer

BleepingComputer получил образец этого ранее неизвестного дампа данных Twitter, который содержит 1 377 132 телефонных номера пользователей во Франции.

С тех пор мы подтвердили многочисленным пользователям в этой утечке, что номера телефонов действительны, подтверждая, что это дополнительное нарушение данных реально.

Кроме того, ни один из этих телефонных номеров не присутствует в исходных данных, проданных в августе, что иллюстрирует, насколько масштабнее была утечка данных Twitter, чем было раскрыто ранее, и большой объем пользовательских данных, циркулирующих среди злоумышленников.

Помпомпурин также подтвердил BleepingComputer, что они не несут ответственности и не знают, кто создал этот недавно обнаруженный дамп данных, что указывает на то, что эту уязвимость API использовали другие люди.

BleepingComputer узнал, что этот недавно обнаруженный дамп данных состоит из множества файлов, разбитых по кодам стран и регионов, включая Европу, Израиль и США.

Нам сказали, что он состоит из более чем 17 миллионов записей, но мы не смогли подтвердить это независимо.

Поскольку эти данные потенциально могут быть использованы для целенаправленных фишинговых атак с целью получения доступа к учетным данным для входа в систему, важно тщательно проверять все электронные письма, которые утверждают, что пришли из Twitter.

Если вы получили электронное письмо, в котором утверждается, что ваша учетная запись была заблокирована, возникли проблемы со входом в систему или вы собираетесь потерять свой подтвержденный статус, и вам предлагается войти в домен, отличный от Twitter, проигнорируйте электронные письма и удалите их как есть. вероятны попытки фишинга…». ***(Lawrence Abrams. 5.4 million Twitter users' stolen data leaked online — more shared privately // Bleeping Computer®***

(https://www.bleepingcomputer.com/news/security/54-million-twitter-users-stolen-data-leaked-online-more-shared-privately/). 27.11.2022).

***

«Экосистема школы сильно отличается от экосистемы типичного предприятия. Перед школьным округом стоит не только монументальная задача по обучению наших подрастающих поколений, но он должен делать это в масштабе предприятия из списка Fortune 500 с небольшой долей бюджета! В связи с ростом числа атак программ-вымогателей администраторы должны найти способы не допустить, чтобы их школы стали следующей жертвой, сохраняя при этом целостность учебного процесса.

Кроме того, в отличие от компаний, которые проводят собеседования и отбирают своих сотрудников, государственные школы K-12 чаще всего не выбирают своих учеников — они должны обучать всех. От тех, кто нуждается в физических приспособлениях или учебных программах, адаптированных к особым потребностям, до тех, кто сталкивается с языковым барьером или другими проблемами, студенческие группы невероятно разнообразны. Добавьте к этому широкий возрастной диапазон от детского сада до старшей школы, и индивидуальные потребности учащихся огромны и постоянно меняются. Наряду с детьми есть роли учителя и персонала, которые могут быть такими же стратегическими, как роль директора, или в последнюю минуту, как роль замещающего учителя. Всем — даже родителям — нужен доступ к технологиям, от которых ежедневно зависит школьная система. Именно этот доступ требует последовательной и мощной защиты.

К сожалению, учащиеся и сотрудники часто становятся уязвимыми из-за повторного использования паролей на десятках платформ, устройств, веб-сайтов и приложений в школе. Согласно недавнему исследованию, 40 процентов школьных округов имеют не менее 10 000 цифровых идентификаторов, при этом большинство пользователей используют шесть или более учетных записей для приложений. Поскольку преподаватели или другие сотрудники не имеют возможности управлять этими цифровыми удостоверениями, это не только открывает двери для дорогостоящих утечек данных, но также может привести к нарушению работы в классе, которое трудно восполнить. Когда сообщается, что другая школа подверглась кибератаке, обычно скомпрометирован пользователь.

Создание двустороннего подхода к безопасности, ориентированного на удостоверения, который включает комплексные программы повышения осведомленности (обучение) и гибкую платформу управления удостоверениями и доступом (IAM), имеет большое значение для устранения этих препятствий, связанных с учетными данными.

Попытка помочь семилетнему ребенку запомнить сложный пароль или директора для отслеживания многочисленных входов в систему может быть сложной задачей, когда проблема множится в классах и офисах. Если школьные округа постоянно отслеживают все цифровые удостоверения с помощью защищенных привилегированных учетных данных и обеспечивают гибкость,

которая диктуется широкими потребностями учащихся и учителей, вся среда поддерживает гораздо более надежную кибербезопасность.

Программы повышения осведомленности для всех

Обучение, посвященное методам социальной инженерии и фишингу, не должно ограничиваться учителями и персоналом. Огромный студенческий состав может служить мощной оборонительной силой. Когда вас учат, на что обращать внимание и чего следует избегать, неизбежно возникает повышенное усердие и меньше шансов нажать на злополучную ссылку или непреднамеренно предоставить кому-либо несанкционированный доступ к учетной записи студента или сотрудника.

Слишком часто школьное ИТ-руководство выделяет больше ресурсов на инициативы по обеспечению безопасности на уровне учителей и персонала, но данные учетных записей учащихся являются столь же конфиденциальными и важными. Вовлекая учащихся почти любого возраста в регулярные занятия, адаптированные к их возрастной группе и использованию технологий, школьная система увеличила количество глаз и ушей, защищающих их школу.

Платформы IAM последовательно обеспечивают безопасность учетных данных

В то время как технологии создали безграничные возможности для обучения, они также создали постоянно растущие проблемы безопасности данных. Дистанционное обучение, облачные инструменты, смартфоны, ноутбуки и бесчисленное множество других устройств стерли с лица земли любой периметр для школ и конфиденциальную информацию, которую они хранят.

В связи с тем, что киберпреступники нацелены на огромное количество потенциальных жертв идентичности в секторе образования, строгая аутентификация и подход с нулевым доверием, ставший возможным благодаря платформам IAM, становятся инструментами для учебных программ. С помощью IAM они защищают время инструкций и снижают вероятность задержек или масштабных сбоев из-за программ-вымогателей.

Повторяющиеся ручные задачи в школьной системе могут быть огромным слабым местом. Благодаря надлежащему управлению жизненным циклом удостоверений с помощью платформы IAM администраторы, ИТ-персонал и студенты, не говоря уже о важных поставщиках и других партнерах, могут безопасно управлять своими учетными записями в соответствии с политиками безопасности. Кроме того, создание/изменение/удаление учетных записей может быть автоматическим, что еще больше снижает вероятность дыр в безопасности. Этот специфический, детальный подход к обеспечению последовательного управления пользователями и группами, возможно, является одной из наиболее очевидных иллюстраций роли IAM как инструмента поддержки в образовании.

Поддержание продуктивности процесса обучения при одновременном повышении безопасности является ключевым моментом при поддержании программы кибербезопасности с учетом бюджета». ***(Michael Webb. Overcoming unique cybersecurity challenges in schools // Help Net Security (https://www.helpnetsecurity.com/2022/11/25/ransomware-attacks-schools/). 25.11.2022).***

***

«Месенджер WhatsApp знову потрапив до скандалу, пов'язаного із безпекою даних. Як стверджує невідомий хакер, дані про майже 500 млн користувачів WhatsApp були вкрадені та виставлені на продаж. В цьому випадку йдеться про номери телефонів, до яких прив'язані облікові записи.

Якщо точніше, зловмисник виставив на продаж базу даних поточного року, що включає інформацію про 487 млн. користувачів WhatsApp з 84 країн світу. Тобто, це майже чверть усіх користувачів месенджера.

Повідомляється, що понад 32 млн. записів від користувачів у США, 11 млн. — від користувачів з Великобританії. Інші країни, де вкрали найбільше номерів, включають Єгипет (45 млн), Італію (35 млн), Саудівську Аравію (29 млн), Францію (20 млн), Туреччину (20 млн) тощо…». ***(Хакери виставили на продаж базу даних користувачів WhatsApp // no worries! (https://noworries.news/hakery-vystavyly-na-prodazh-bazu-danyh-korystuvachiv-whatsapp/). 26.11.2022).***

***

«Кража учетных данных — это вид кибератаки, при которой целью хакера становится программа, управляющая безопасностью Windows. Эта программа хранит информацию для входа в систему, которую можно сравнить с ключами от дома: если украсть их и сделать копию, то доступ к жилью будет открыт в любое время.

Представляем подробный разбор кражи учетных данных на Windows: как она происходит, по каким признакам определяется и как ее избежать.

Что такое LSASS на Windows

Сервис проверки подлинности локальной системы безопасности (Local Security Authority Server Service, LSASS) — это процесс, который управляет политикой безопасности компьютера. LSASS проверяет логины, изменения паролей, токены доступа и административные привилегии у пользователей системы или сервера.

LSASS можно сравнить с охранником, который проверяет документы на входе в ночной клуб. Без него в заведение смог бы попасть любой человек с поддельными документами.

Стать востребованным специалистом по кибербезопасности можно, выбрав онлайн-курс в каталоге курсов по информационной безопасности.

LSASS выполняется как процесс под названием lsass.exe. При запуске lsass.exe хранит в памяти такие аутентификационные данные, как зашифрованные пароли, HT-хэши, LM-хэши и билеты Kerberos. Благодаря этому пользователи могут работать с файлами во время активных сеансов Windows, не вводя учетные данные каждый раз, когда нужно выполнить какую-либо задачу.

При краже учетных данных злоумышленники удаляют, перемещают, редактируют или заменяют настоящий файл lsass.exe. Для этого обычно используются такие инструменты, как Mimikatz, Crackmapexec и Lsassy.

Как происходит кража учетных данных через LSASS

Для этого злоумышленники обычно получают удаленный доступ к компьютеру жертвы — это можно сделать несколькими способами.

Во-первых, хакеру нужно получить права администратора, чтобы изменять LSASS. Так он сможет установить вредоносное ПО, чтобы скопировать данные процесса LSASS, скачать эту копию и локально извлечь из нее учетные данные.

Однако, поскольку антивирус Microsoft Defender обнаруживает и удаляет вредоносное ПО все эффективнее, хакеры все чаще применяют тактику Living off the Land, при которой атаки совершаются через предустановленные программы.

Признаки кражи учетных данных

Эти пять способов помогут выяснить, не стали ли вы жертвой хакерской атаки.

Lsass.exe использует много аппаратных ресурсов

Откройте «Диспетчер задач» и проверьте, сколько CPU и памяти использует этот процесс. В обычных условиях он потребляет 0% CPU и около 5 МБ памяти. Стоит насторожиться, если он сильно нагружает CPU и задействует более 10 МБ, а вы за последнее время не выполняли никаких действий, связанных с безопасностью, например не меняли данные для входа.

В таком случае завершите процесс через «Диспетчер задач». Затем откройте местоположение файла и удалите его. В отличие от поддельного, реальный процесс отобразит ошибку. Помимо этого, стоит заглянуть в «Историю файлов» и проверить, не сохранила ли Windows резервную копию процесса.

В названии процесса есть ошибки

Хакеры часто переименовывают взломанные процессы так, чтобы они выглядели как настоящие. В таком случае злоумышленник может использовать заглавную «i», чтобы имитировать «L» в аббревиатуре LSASS. Обнаружить такое название можно с помощью конвертера регистров.

В названии также могут присутствовать лишние «a» и «s». Если вы встретили подобный файл, то удалите его (а также его резервные копии из «Истории файлов»).

Lsass.exe находится в другой папке

Снова откройте «Диспетчер задач», пролистайте до «Процессы Windows» и найдите Local Security Authority Process. Затем нажмите на него правой кнопкой мыши и выберите «Открыть расположение файла».

Настоящий файл lsass.exe находится в папке C:\Windows\System32. Если он расположен в любом другом месте, то это, скорее всего, вредоносное ПО, и его стоит удалить.

В «Диспетчере задач» есть более одного процесса Lsass

В «Диспетчере задач» должен отображаться лишь один Local Security Authority Process. При открытии выпадающего меню, расположенного слева от названия процесса, появляется список активных служб — это тоже нормально.

Однако если вы обнаружили несколько процессов LSASS, а также более одного lsass.exe при открытии расположения файла, то велика вероятность, что ваш компьютер подвергся атаке хакеров. Попробуйте удалить эти файлы — если это настоящий lsass.exe, появится ошибка.

Файл Lsass.exe весит слишком много

Объем файлов lsass.exe небольшой: примерно 83 КБ на компьютере на базе Windows 11 и 60 КБ — на Windows 10. Конечно, хакеры понимают, что большой lsass.exe сразу привлечет внимание владельца устройства, поэтому обычно

стараются этого избегать. Тем не менее, если учесть приведенные выше сигналы, вредоносное ПО все равно удастся обнаружить.

Способы предотвратить кражу учетных данных через LSASS

Безопасность на компьютерах Windows постепенно улучшается, но кража учетных данных остается серьезной угрозой. Особенно это актуально для старых устройств, работающих на устаревших операционных системах, и новых, не получающих обновления ПО.

Ниже представлены три простых способа избежать этой угрозы.

Установите последние обновления системы безопасности

Такие обновления исправляют уязвимости, которые злоумышленники могут использовать для атаки на компьютер. Поддержание устройств в актуальном состоянии снижает риск взлома. Для этого подключите автоматическую загрузку и установку обновлений для Windows, а также сторонних программ, установленных на ПК.

Используйте Credential Guard в Защитнике Windows

Credential Guard или Диспетчер учетных данных — это механизм безопасности, создающий изолированный процесс LSASS (LSAIso), который безопасно хранит все учетные данные и взаимодействует с основным LSASS для проверки пользователей. Этот механизм защищает целостность личной информации и предотвращает ее кражу.

Credential Guard доступен на корпоративной и профессиональной версиях Windows 10 и 11, а также на некоторых версиях серверных ОС Windows Server. Устройства также должны соответствовать строгим требования, таким как наличие протокола Secure Boot и поддержка 64-разрядной виртуализации. Эта функция не активирована по умолчанию — ее нужно устанавливать вручную.

Отключите удаленный доступ к рабочему столу

С помощью удаленного доступа вы и другие авторизованные пользователи можете использовать компьютер, находясь в другом физическом месте. Эта функция позволяет вам переносить файлы с рабочего на домашнее устройство, а сотрудникам техподдержки — удаленно устранять неполадки. Это удобно, но делает компьютер уязвимым для хакерских атак.

Чтобы отключить удаленный доступ, нажмите клавишу «Пуск» и введите в поисковую строку «удаленный доступ». Выберите «Разрешить удаленные подключения к этому компьютеру» и уберите галочку у пункта «Разрешить подключение удаленного помощника к этому компьютеру».

Помимо этого, можно удалить ПО для удаленного доступа, такое как TeamViewer, AeroAdmin и AnyDesk. Эти программы повышают риски, в том числе, атак в стиле Living off the Land». ***(Дарья Сидорова. Что такое кража учетных данных и как предотвратить ее на Windows // РБточкаРУ (https://rb.ru/story/attack-on-windows/). 23.11.2022).***

***

«У Великій Британії жінка подала до суду на Facebook. Позивачка вважає, що компанія Meta нехтує правом виступати проти збору її особистих даних.

Про це пише видання The Guardian.

Деталі

Як повідомляє The Guardian, позивачка Таня О'Керролл звинувачує Meta в тому, що та порушила закони Великої Британії про дані. Зокрема, жінка вимагає, аби соціальна мережа Facebook припинила збір та обробку її даних.

Як відомо, Facebook отримує прибуток від реклами, яку спрямовує своїм користувачам з урахуванням їх конкретних інтересів та походження.

О'Керролл стверджує, що Facebook порушив статтю 21 Загального регламенту захисту даних Великої Британії, яка дає людям право протестувати проти обробки своїх персональних даних у маркетингових цілях. О'Керролл сказала, що успішна справа може створити прецедент для мільйонів користувачів Facebook, соціальних мереж та пошукових систем.

«У цьому випадку я дійсно використовую це право, яке давно було в законах, але досі не використовувалося, тобто право просто сказати: «Я заперечую», — сказала позивачка.

Відомо, що жінка вже подала відповідний позов до Високого суду і вимагає не відшкодування збитків, а можливості свого вибору "так або ні".

Реакція керівництва Meta

Своєю чергою, у компанії Meta заявляють, що для них конфіденційність клієнтів понад усе. Мовляв, у компанії спеціально розробили інструменти, які допомагають людям контролювати, яку рекламу вони можуть отримувати, мовляв, це зовсім не означає, що за ними хтось стежить.

«Ми знаємо, що конфіденційність важлива для наших користувачів, і ставимося до цього серйозно. Ось чому ми створюємо такі інструменти, як перевірка конфіденційності та рекламні уподобання, де ми пояснюємо, якими даними люди поділилися, і показуємо, як вони можуть контролювати тип реклами, яку вони бачать», — заявив представник Meta». ***(Facebook звинувачують у стеженні за користувачами: подробиці // Internetua (https://internetua.com/facebook-zvinuvacsuuat-u-stejenni-za-koristuvacsami-podrobici). 23.11.2022).***

***

«Група спостерігачів за технологічною платформою повідомила, що виявила понад 100 груп у Facebook, деякі з яких мають десятки тисяч членів, де облікові записи для управління бізнесом купуються та продаються з порушенням правил соціальної мережі.

Облікові записи можна використовувати для запуску кількох сторінок і рекламних кампаній, створюючи нові можливості для онлайн-шахрайства, дезінформації та втручання у вибори, згідно з розслідуванням Tech Transparency Project, вашингтонської інформаційної та дослідницької організації, яка зосереджується на вплив основних технологічних платформ на суспільство.

«Роками Facebook стверджував, що його системи штучного інтелекту можуть очистити його платформу, але знову і знову ми виявляли, що технологія Facebook не в змозі видалити шкідливий контент, який порушує його політику», — сказала TechNewsWorld директор TTP Кеті Пол. «Це, на жаль, також стосується чорного ринку рекламних облікових записів».

ТТР пояснив, що облікові записи бізнес-менеджерів дозволяють менеджерам соціальних мереж і маркетологам керувати колекцією рекламних облікових записів Facebook, сторінок Facebook і облікових записів Instagram з однієї інформаційної панелі. Він додав, що материнська компанія Facebook Meta рекламує їх як «єдиний магазин» для реклами та маркетингу на своїх платформах.

У звіті стверджується, що облікові записи є особливо цінними для шахраїв, оскільки керівники компаній можуть запускати серію рекламних кампаній і легко додавати нових користувачів і рекламні облікові записи для розширення свого охоплення.

У групах Facebook, перевірених ТТР, група зазначила, що користувачі часто продають акаунти великими партіями. Багато облікових записів пов'язано з чиєюсь кредитною карткою, вказує на те, що їх зламали або вкрали. «Це, очевидно, є великою проблемою для окремих користувачів або малих підприємств, у яких неавторизована особа раптом стягує великі витрати з їхньої картки», — сказав Пол.

У звіті також виявлено, що в деяких випадках продавці пропонують облікові записи, схвалені для реклами політичних, виборчих і соціальних питань.

Facebook Acts

Отримавши попередження про ситуацію, Facebook почав демонтаж чорного ринку. «Ми видалили групи, які були позначені до нас минулого тижня за порушення нашої політики, і ми продовжимо переглядати додаткові групи та видаляти ті, які порушують» - йдеться в заяві компанії, наданій TechNewsWorld речником Ерін Макпайк.

Окрім видалення груп, компанія заявила, що встановила контрольні точки для кількох адміністраторів груп, вимагаючи надання додаткової інформації, перш ніж вони зможуть отримати доступ до своїх облікових записів.

Незважаючи на дії Facebook, у звіті стверджується, що чорний ринок викликає деякі тривожні питання для компанії та її материнської компанії Meta. Враховуючи давню проблему Facebook із шахрайською рекламою та історію втручання Росії у вибори, незрозуміло, чому Meta не робить більше для боротьби з цією незаконною торгівлею, зазначається у звіті». ***(Дмитро Сизов. Watchdog виявив у Facebook процвітаючий чорний ринок шахрайських рекламних облікових записів // Internetua (https://internetua.com/watchdog-viyaviv-u-facebook-procvitauacsii-csornii-rinok-shahraiskih-reklamnih-oblikovih-zapisiv). 26.11.2022).***

***

«Хакеры взломали и «слили» данные 7 млн пользователей Twitter: чем это грозит людям

Злоумышленник воспользовался уязвимостью, чтобы получить номера телефонов и email, а затем продать их за $30 тыс. Затем его методом воспользовались другие.

Хакеры разместили в открытом доступе закрытую информацию о 7 миллионах аккаунтов Twitter. Подробности сообщает портал Bleeping Computer.

Исследователи из сферы кибербезопасности обнаружили на хакерском форуме Breached крупную базу данных, в которой помимо общедоступных данных содержатся номера телефонов и адреса электронной почты — эта информация о

пользователях должна оставаться закрытой. Как утверждает автор поста с ником devil, информация касается 5,4 млн разных людей и организаций, в том числе крупных компаний и знаменитостей. В августе выставил базу на продажу, оценив ее в $30 тыс., а в сентябре и ноябре она оказалась в открытом доступе.

«Я только что получил доказательства массовой утечки, затронувшей миллионы учетных записей Twitter в ЕС и США. Я связался с несколькими пользователями, и они подтвердили, что утекшие данные верны. Это нарушение произошло не ранее 2021 года», — написал в Twitter эксперт по кибербезопасности Чад Лодер, приведя в доказательство фрагмент базы данных.

Преступники могут использовать номера телефонов и e-mail для целенаправленных фишинговых атак с целью получения доступа к учетным данным для входа в систему, поэтому пользователям Twitter следует осторожно открывать подозрительные электронные письма, особенно от самой социальной сети. К примеру, мошенники могут прислать сообщение о блокировке аккаунта и предложить перейти на сторонний сайт, чтобы получить деньги или информацию для взлома других учетных записей.

Как позже выяснили специалисты, хакеры получили данные в декабре 2021 года благодаря уязвимости Twitter API, раскрытой в рамках проекта HackerOne, где специалисты обнаруживали ошибки за вознаграждение. Лазейка позволяла отправлять номера телефонов и адреса электронной почты в программный интерфейс соцсети для получения связанного с ними идентификатора Twitter. Используя этот идентификатор, хакеры могут получить как общедоступную, так и конфиденциальную информацию из учетной записи.

BleepingComputer выяснил, что несколько злоумышленников использовали уязвимость для кражи личной информации из Twitter, однако неизвестно, была ли она раскрыта участниками HackerOne. Журналисты поделились образцом записей с представителями Twitter, и компания подтвердила утечку данных, отметив, что ошибку исправили в январе 2022 года.

Владелец хакерского форума Breached сообщил BleepingComputer, что его команда узнала об уязвимости благодаря хакеру devil, а затем использовала ее для создания большой базы данных. Помимо 5,4 млн, они собрали еще 1,4 млн заблокированных аккаунтов, собранных с использованием других инструментов, которые не продали, но передали некоторым людям в частном порядке.

BleepingComputer получил образец нового набора данных, включающий более 1,3 млн телефонных номера из Франции. Издание связалось с пользователями и подтвердило актуальность слитых данных. При этом ни одного из этих номеров нет в первоначальной базе, проданной в августе 2022 года. Новая база разбита на отдельные файлы по кодам стран и регионов, например, в ней есть данные жителей Израиля, США и Европы». ***(Хакеры взломали и «слили» данные 7 млн пользователей Twitter: чем это грозит людям // ФОКУС (https://focus.ua/digital/538912-hakery-vzlomali-i-slili-dannye-7-mln-polzovateley-twitter-chem-eto-grozit-lyudyam). 29.11.2022).***

***

«Благодаря современным передовым технологиям лицевая биометрия теперь является шлюзом для компаний, позволяющим проверять личность своих клиентов с высокой степенью достоверности, а также обеспечивает простой и оптимизированный пользовательский интерфейс.

Мнения, выраженные участниками Entrepreneur, являются их собственными.

Использование лица человека для аутентификации — это то, чем люди занимались сотни тысяч лет. Новые технологические достижения изменили то, как мы взаимодействуем друг с другом, и предприятия особенно извлекают выгоду из этих достижений для проверки личности. Предыдущие столпы личной и цифровой проверки, такие как проверка подлинности на основе знаний (KBA), больше не являются адекватной защитой от мошенничества.

Почему? Вместе с развитием технологий развивается и мошенничество. Технология лицевой биометрии стала основой, на которую полагаются предприятия и потребители для проверки своей личности. В этой статье мы приведем пять основных причин, по которым биометрия лица может помочь вашему бизнесу.

1. Это очень точно и может остановить мошенничество

Биометрия лица дает предприятиям высокую степень уверенности в том, что клиент является законным пользователем и является тем, за кого себя выдает. Процесс аутентификации оптимизирован так, как никогда не могли бы быть пароли и традиционная двухфакторная аутентификация (2FA): все, что нужно сделать пользователям, это посмотреть на свое устройство или любую другую камеру, чтобы подтвердить свою личность.

Помимо того, что мошенникам очень трудно скомпрометировать данные из-за точности технологии распознавания лиц, передовые алгоритмы также теперь дают почти нулевую систематическую ошибку, работая намного лучше, чем ручной просмотр человеком. Фактически, в одном недавнем исследовании алгоритмов распознавания лиц NIST обнаружил, что технология может идентифицировать пассажиров, садящихся в самолет, с точностью 99,5%. Кроме того, этот показатель успеха (для лучших алгоритмов распознавания лиц) был одинаковым независимо от демографии, а это означает, что раса или пол не оказывали существенного влияния на точность.

Такой уровень точности может существенно повлиять на способность бизнеса бороться с различными видами мошенничества. Например, при создании учетной записи компании могут быть гораздо более уверены в том, что пользователь настоящий, благодаря подтверждению личности (при условии, что они сопоставляют селфи с обнаружением живости и подлинным государственным удостоверением личности). Это также может предотвратить мошенничество с захватом учетной записи; Двухфакторную аутентификацию на основе SMS, как известно, легко перехватить, а современные алгоритмы все лучше справляются с отсеиванием сложных 3D-масок или подобных хакерских приемов спуфинга лиц.

2. Это просто для пользователей

Пользователям также несложно внедрить биометрию лица. Клиентов легко отключить неуклюжими мерами аутентификации, такими как KBA, особенно если они требуются несколько раз во время транзакции. Гораздо проще посмотреть в

камеру и сделать селфи вместо того, чтобы вводить пароль или получать текстовое сообщение.

Биометрия лица также получает все более широкое признание среди населения в целом. По мере того, как проблемы с конфиденциальностью и точностью устраняются и исправляются, эта технология будет продолжать получать широкое признание. Хотя использовать любой метод биометрии лучше, чем не использовать его вообще, есть причина, по которой все наши устройства перешли на биометрию лица для разблокировки: проще говоря, это проще для пользователя. Компании могут воспользоваться этим растущим признанием и сделать работу пользователей проще и безопаснее всего одним шагом, что сделает клиентов более довольными.

3. Это обеспечивает надежный андеррайтинг

Все больше и больше компаний прибегают к жестким методам андеррайтинга для борьбы с мошенничеством и соблюдения нормативных требований. Дружеское мошенничество дорого обходится современному бизнесу. К сожалению, мошенники могут попытаться заявить о законной покупке, продлении подписки или изменении учетной записи мошенническим путем и запросить возврат платежа. Продавцы в подавляющем большинстве несут бремя этого мошенничества, когда они не могут подтвердить личность, но распознавание лиц может значительно уменьшить его количество.

Точно так же, как наличие свидетеля на месте преступления, биометрия лица предоставляет предприятиям подтвержденное изображение человека, совершающего транзакцию, с отметкой времени. Когда кто-то пытается оспорить обвинение, у этой компании есть неопровержимые доказательства того, что это лицо действительно совершило покупку. Это также важно для соблюдения нормативных требований и даже для защиты бизнеса от штрафов и судебных исков. Он также предоставляет надежные доказательства в случае любых будущих проверок учетной записи клиента или истории покупок.

4. Это может снизить эксплуатационные расходы

Биометрия лица может снизить эксплуатационные расходы за счет устранения необходимости в текущих трудоемких проверках безопасности, которые используются для подтверждения личности клиента в случае подозрительных покупок, электронных переводов или изменений в счете. Это включает в себя текстовые или электронные письма клиенту, а также даже звонки им, чтобы убедиться, что они стоят за событием. Эти расходы на обслуживание клиентов могут быстро возрасти, не говоря уже о том, что вы повышаете вероятность того, что ваши пользователи столкнутся с плохим обслуживанием клиентов, а также открываете свой бизнес для мошенничества с помощью атак типа «человек посередине».

Кроме того, увеличилось количество аналитиков, необходимых для проверки, мониторинга и даже исправления транзакций. Исследование LexisNexis True Cost of Fraud Study 2022 года теперь подсчитало, что каждый доллар убытков от мошенничества фактически обходится бизнесу в 3,75 доллара из-за увеличения объема мошенничества, новых цифровых способов оплаты и высокой стоимости замены и перераспределения товаров.

Биометрия лица делает все это ненужным. Компании могут сократить значительные операционные расходы и сэкономить время и ресурсы для своих групп

по борьбе с мошенничеством, просто сочетая быстрое селфи с обнаружением живости. Вы можете быть уверены с высокой степенью уверенности в том, что человек является тем, кем он себя называет, и ваша команда может перестать тратить время на анализ транзакций или разблокировку учетных записей.

5. Устройство не зависит

Наконец, биометрию лица можно внедрить, не заботясь об устройствах клиентов, поскольку она не зависит от устройства. Пока на устройстве есть камера, оно может выполнять необходимые функции для аутентификации по лицу. Нет необходимости в сканерах отпечатков пальцев или микрофонах в шумных и оживленных местах; эти камеры маленькие, недорогие и могут быть установлены в любом киоске, где происходят такие сделки. Кроме того, даже дешевые камеры могут обеспечить точное распознавание лиц с помощью современных алгоритмов. Также помогает то, что почти каждый носит высококачественную камеру в кармане через свое мобильное устройство.

Люди используют распознавание лиц, чтобы идентифицировать других каждый день. Это был странный век, когда наш переход к цифровым технологиям быстро опередил технологии, позволяющие продолжать использовать лица. Однако мы быстро преодолели это ограничение, и биометрия лица стала для компаний надежным средством проверки личности своих клиентов. Пришло время сделать шаг, и компании, которые смогут полностью внедрить аутентификацию по лицу, пожнут плоды». ***(Clayton Roth. Top 5 Reasons Facial Biometrics Can Help Your Business // Entrepreneur Media, Inc (https://www.entrepreneur.com/science-technology/5-ways-facial-biometrics-can-help-your-business/438479). 28.11.2022).***

***

«Известная платформа коротких видео ByteDance, TikTok, являющаяся одним из самых быстрорастущих приложений, теперь находится под пристальным вниманием хакеров для проведения своих вредоносных кампаний.

Согласно последнему отчету Checkmarx, компании, занимающейся кибербезопасностью, дикая тенденция TikTok «Невидимый вызов» используется хакерами, чтобы заманивать жертв с помощью вредоносных программ и получать доступ к их файлам, включая сохраненные в Интернете учетные данные для других приложений, таких как Discord или кошельки виртуальной валюты.

Тенденция побуждает пользователей ходить полностью обнаженными и размывать свое тело с помощью невидимого фильтра тела; хакеры пользуются этим и предлагают программное обеспечение, которое может удалить эффект фильтра, чтобы они могли получить в свои руки TikTok с обнаженными телами.

Но на самом деле это просто ловушка, расставленная оператором вредоносного ПО, поскольку они маскируют вредоносное ПО под фильтр, и всякий раз, когда пользователь его устанавливает, данные скомпрометированы.

TikTok использовался для распространения вредоносного ПО. Две учетные записи, которые позже были удалены регуляторами приложений, опубликовали короткое видео, рекламирующее очевидный взлом удаления фильтра. Учетные записи совместно использовали дескриптор Discord для сервера, через который

пользователи могли установить ошибку. Согласно отчету, на сервере Discord до его удаления было почти 32 тысячи пользователей.

Вредоносное ПО состоит из двух файлов, командного файла и файла readme, которые были дополнительно связаны каналом YouTube, на котором размещено руководство по всему процессу.

Согласно отчету, несмотря на то, что вредоносные кампании удалялись несколько раз, они все еще продолжаются, поскольку человек, стоящий за ними, продолжает изменять код различными способами. В отчете также прогнозируется, что этот тип злонамеренной кампании резко возрастет в следующем году.

Ожидается, что хакеры изменили свою кампанию с предложения фильтров, которые удаляют фильтры размытия, на другие предложения, которые могут привлечь больше пользователей к фальсифицированному программному обеспечению.

Хотя связанные с ним серверы были удалены соответствующими властями, группа, стоящая за ним, продолжает создавать новые группы и серверы для проведения своей кампании». ***(Arooj Ahmed. Hackers are targeting the "Invisible Body" trend on TikTok to spread malicious software // Digital Information World (https://www.digitalinformationworld.com/2022/11/hackers-are-targeting-invisible-body.html). 30.11.2022).***

***

Кіберзлочинність та кібертерроризм

«Предполагаемый хакер переместил средства через Binance, Coinbase и 4 другие биржи

Британский суд обязал шесть криптовалютных бирж раскрыть личности владельцев счетов, предположительно связанных со взломом анонимной английской криптовалютной платформы в 2020 году, в ходе которого воры украли цифровые активы на сумму 10,7 млн долларов.

Биржи должны делиться статусом украденных средств, данными «знай своего клиента» предполагаемых хакеров, а также данными их банковских счетов и платежных карт, адресами электронной почты, адресами проживания, номерами телефонов и банковскими выписками, постановил судья Высокого суда Кристофер Батчер.

Его приказ во вторник от имени истца, личность которого не разглашается — истец выступает в суде под псевдонимом LMN и не связан с одноименной коллекцией мультяшных лимонов NFT — предписывает биржам сотрудничать без «неизбежной задержки». Это биржи Binance, Bitflyer, Payward, которая работает как Kraken, Luno PTE, Coinbase Global и Huobi Global.

Компания-жертва сначала связалась с правоохранительными органами, а затем наняла эксперта по криптовалюте для отслеживания украденных средств. Это расследование зашло в тупик с платформами, поскольку адреса кошельков, которые обнаружил следователь, были омнибусными счетами, используемыми платформами для управления сделками нескольких лиц.

Сайед Рахман, партнер юридической фирмы Rahman Ravelli, подавший иск от имени платформы-жертвы, сообщил Information Security Media Group, что эксперт «проследил активы на 1,7 миллиона долларов до 26 счетов, все из которых принадлежали или управлялись одним из шести обмены под вопросом».

Он назвал решение Мясника «вехой», предупреждающей воров криптовалюты о том, что суды «помогут отдельным лицам и компаниям отследить и вернуть украденные активы».

Ари Редборд, бывший старший советник Министерства финансов по борьбе с отмыванием денег и сотрудник ISMG, сказал: «Будет интересно посмотреть, как в этом случае отреагируют биржи». По его словам, большинство из них, скорее всего, отреагируют на постановление суда. «Тем не менее, трудно обеспечить соблюдение судебного процесса за пределами юрисдикции. Поэтому, если биржа решит не подчиняться требованиям, обеспечение соблюдения может стать проблемой».

Биржи, в том числе Coinbase, которые активно участвовали в слушаниях 11 ноября, приведших к приказу, не ответили на запрос о комментариях, в том числе о том, намерены ли они выполнить приказ Мясника.

Британский судья издал приказ, несмотря на то, что биржи находятся за пределами Соединенного Королевства, сославшись на обновление гражданского процессуального законодательства от октября 2022 года, которое упростило приказы о раскрытии информации в отношении иностранных организаций в случаях мошенничества, которые должны были рассматриваться в английских или валлийских судах.

По словам Рахмана, до обновления было «намного сложнее» вызывать в суд платформы для торговли криптовалютами, базирующиеся за пределами Великобритании. По его словам, это особенно усложнило ведение гражданских дел против мошенничества с криптовалютой.

Рахман сказал, что ожидает, что Высокий суд назначит последующее слушание, чтобы гарантировать, что биржи получат надлежащее уведомление о приказе». ***(Rashmi Ramesh. UK Court Orders Crypto Firms to Share Data to Track Thieves // Information Security Media Group, Corp. (https://www.govinfosecurity.com/uk-court-orders-crypto-firms-to-share-data-to-track-thieves-a-20589). 30.11.2022).***

***

«Услуги от дочерней компании Boeing Jeppesen, пострадавшей от продолжающегося инцидента

Дочерняя компания Boeing, которая распространяет уведомления о безопасности воздушного пространства среди пилотов, переживает второй день простоев, вызванных инцидентом с кибербезопасностью.

Jeppesen, которая предоставляет электронные уведомления для бюллетеней о воздушных миссиях и приложений для задач управления в полете, «в настоящее время испытывает технические проблемы с некоторыми из наших продуктов, услуг и каналов связи», как говорится в баннере на ее веб-сайте.

Техническая проблема связана с киберинцидентом, природу которого Boeing не раскрывает. Одним из последствий сбоя является получение и обработка уведомлений.

«В настоящее время у нас нет оснований полагать, что этот инцидент представляет угрозу безопасности самолетов или полетов», — заявил представитель компании Information Security Media Group.

Boeing общается с клиентами и регулирующими органами и в настоящее время работает над восстановлением полного сервиса «как можно скорее».

Альтернативные источники уведомления о воздушной миссии включают Федеральное авиационное управление США и Международную организацию гражданской авиации.

На авиационный сектор приходится большая доля кибератак. В октябре пророссийская политическая хакерская группа взяла на себя ответственность за распределенные атаки типа «отказ в обслуживании», которые отключили общедоступные веб-сайты нескольких крупных аэропортов США.

Европейская организация по безопасности аэронавигации в отчете за июль 2021 года обнаружила значительный рост числа киберинцидентов в этом секторе, в основном в авиакомпаниях. «Атаки происходят во всех категориях угроз, и только более качественная отчетность не полностью объясняет 530-процентный рост числа зарегистрированных инцидентов в годовом исчислении», — говорится в нем.

По данным организации, которая координирует воздушное движение в Европе, авиационная отрасль сталкивается с атаками программ-вымогателей со скоростью одна в неделю.

В мае индийская пассажирская авиакомпания SpiceJet заявила, что попытка атаки программы-вымогателя привела к задержкам в обслуживании.

В прошлом SpiceJet сталкивалась с проблемами кибербезопасности. В феврале 2020 года исследователь безопасности взломал систему SpiceJet и получил доступ к незашифрованному файлу резервной копии базы данных, который содержал личную информацию более чем 1,2 миллиона пассажиров.

Boeing также пережил свою долю кибератак, в том числе заражение в 2018 году червем-вымогателем WannaCry. Представитель компании сообщил Seattle Times, что инфекция имеет ограниченный эффект. «Мы установили исправления для программного обеспечения. Программа 777 Jet или любая из наших программ не прерывалась», — сказала она». ***(Prajeet Nair. Cyberattack at Boeing Disrupts Flight Planning // Information Security Media Group, Corp. (https://www.govinfosecurity.com/cyberattack-at-boeing-disrupts-flight-planning-a-20419). 04.11.2022).***

***

«Агентство безопасности заявляет, что 18 инцидентов в 2022 году требовали смягчения последствий, скоординированных на национальном уровне

Атаки программ-вымогателей на британские больницы и школы оставались самой большой угрозой кибербезопасности, с которой столкнулась страна в 2022

году, предупреждает агентство по кибербезопасности страны, добавляя, что в ближайшие месяцы эти атаки, вероятно, усилятся.

В то время как в Соединенном Королевстве наблюдался всплеск различных атак, в том числе низкоуровневых тактик, таких как целевой фишинг, атаки программ-вымогателей на ее критическую инфраструктуру продолжались в течение года, при этом 18 инцидентов в стране потребовали координации на национальном уровне для снижения вредоносного ПО из систем.

К ним относятся нападения на поставщика национальной службы экстренной помощи страны и компанию водоснабжения в Южном Стаффордшире, согласно отчету о киберугрозах за 2022 год, опубликованному Национальным центром кибербезопасности.

NCSC связывает всплеск атак программ-вымогателей с распространением групп программ-вымогателей как услуги, которые, по его словам, расширяют возможности злоумышленников с более низкой квалификацией и членов групп, которым обычно не хватает опыта для развертывания сложных вредоносных программ. По словам NCSC, эти сервисы открыли несколько векторов атак для более широкого круга хакеров.

Кроме того, менее опытные хакеры теперь вооружаются передовым программным обеспечением для вторжений, таким как шпионское ПО военного уровня и готовые продукты для кибер-наблюдения, которые легко доступны на различных рынках киберпреступности. Эти возможности «уменьшили проникновение в киберпреступность» и будут напрямую способствовать вымогательству программ-вымогателей и корпоративному шпионажу против британских предприятий.

«Программы-вымогатели остаются самой серьезной угрозой, с которой сталкиваются предприятия и организации в Великобритании. Эти атаки имеют реальные последствия, и очень важно, чтобы организации относились к ним как к реальным рискам на уровне совета директоров, которым можно управлять», — говорит Линди Кэмерон, генеральный директор Национальный центр кибербезопасности.

Агентство добавляет, что обнаружение в 2021 году уязвимости Log4J, которую хакеры-вымогатели начали активно использовать в качестве оружия в течение нескольких месяцев после ее раскрытия, является еще одним важным вектором атаки, способствующим росту атак программ-вымогателей. Уязвимость JavaScript влияет на несколько версий программного обеспечения и позволяет удаленно выполнять код при использовании.

TellYouThePass, Conti и Khonsari входят в число групп вымогателей, которые успешно использовали Log4j в качестве оружия для нападения на жертв по всему миру.

NCSC также заявляет, что геополитическая напряженность, связанная с российским вторжением в Украину, является еще одним фактором роста числа атак программ-вымогателей.

«Большинство преступных группировок, занимающихся программами-вымогателями, нацеленными на Великобританию, по-прежнему базируются в России и вокруг нее», — говорится в сообщении NCSC. «Хотя неясно, в какой

степени Кремль руководит этими группами вымогателей, те, кто действует внутри границ России, получают выгоду от молчаливого согласия российского государства».

В большинстве атак программ-вымогателей, наблюдавшихся в Великобритании в прошлом году, хакеры в основном полагались на модель вымогательства данных, чтобы заставить жертв платить больше выкупа. В ответ NCSC призывает предприятия и других жертв программ-вымогателей не платить выкуп, чтобы предотвратить будущие атаки». ***(Akshaya Asokan. Ransomware Attacks Pose Biggest Threat to UK Organizations // Information Security Media Group, Corp. (https://www.govinfosecurity.com/ransomware-attacks-pose-biggest-threat-to-uk-organizations-a-20385). 01.11.2022).***

***

«Дерек Манки о том, как киберпреступность как услуга сделает возможными более разрушительные атаки

Дерек Манки, главный стратег безопасности и вице-президент по анализу глобальных угроз, FortiGuard Labs, Fortinet

Конвергенция ландшафта угроз имеет большое значение для защитников, а киберпреступность как услуга потенциально позволит проводить более масштабные разрушительные атаки. Это один из прогнозов ландшафта угроз на 2023 год Дерека Манки из FortiGuard Labs компании Fortinet. Этими и другими наблюдениями он делится.

В видеоинтервью с Information Security Media Group Манки обсуждает:

Общие тренды на новый год;

Что на самом деле означает конвергенция ландшафта угроз;

Три элемента, которые киберзащитники должны учитывать при добавлении в свои портфели безопасности.

Манки формулирует стратегию безопасности. Он имеет более чем 16-летний опыт работы в области кибербезопасности, и его конечная цель — внести позитивный вклад в глобальную войну с киберпреступностью. Манки является лидером отрасли и представляет исследования и стратегии по всему миру на ведущих конференциях по безопасности. Он встречается с ведущими политическими деятелями и ключевыми заинтересованными сторонами, включая правоохранительные органы, и активно участвует в нескольких глобальных инициативах по разведке угроз, включая NICP НАТО, рабочую группу экспертов Интерпола, рабочий комитет Альянса по киберугрозам и FIRST — все в попытке сформировать будущее действенной аналитики угроз и упреждающей стратегии безопасности». ***(Tom Field. FortiGuard Labs: 2023 Threat Landscape Insights // Information Security Media Group, Corp. (https://www.govinfosecurity.com/fortiguard-labs-2023-threat-landscape-insights-a-20430). 07.11.2022).***

***

«Банки в Африке являются основными целями, а средства рассредоточиваются с использованием денежных мулов

Франкоязычная банда была замешана в краже не менее 11 миллионов долларов, в основном из банков в Африке.

Преступный синдикат под кодовым названием Opera1er остается «активным и опасным», согласно новому отчету фирмы по кибербезопасности Group-IB и Координационного центра CERT французского многонационального телекоммуникационного гиганта Orange.

«Исследователи назвали банду Opera1er в честь учетной записи электронной почты, часто используемой бандой для регистрации своих доменов», — сообщает Group-IB, добавляя, что банда также известна как Desktop-Group и NXSMS, а Общество всемирных межбанковских финансовых телекоммуникаций — также известное как SWIFT - в 2020 году получил название Common Raven.

«В период с 2018 по 2022 год банде удалось украсть не менее 11 миллионов долларов, а реальная сумма ущерба может достигать 30 миллионов долларов», — сообщает Group-IB. Среди жертв были фирмы, предоставляющие финансовые услуги, и телекоммуникационные компании в Аргентине, Бангладеш, Буркина-Фасо, Камеруне, Габоне, Кот-д'Ивуаре, Мали, Нигере, Нигерии, Парагвае, Сенегале, Сьерра-Леоне, Того и Уганде. Исследователи говорят, что группа предпочитает бить жертв по выходным или в праздничные дни.

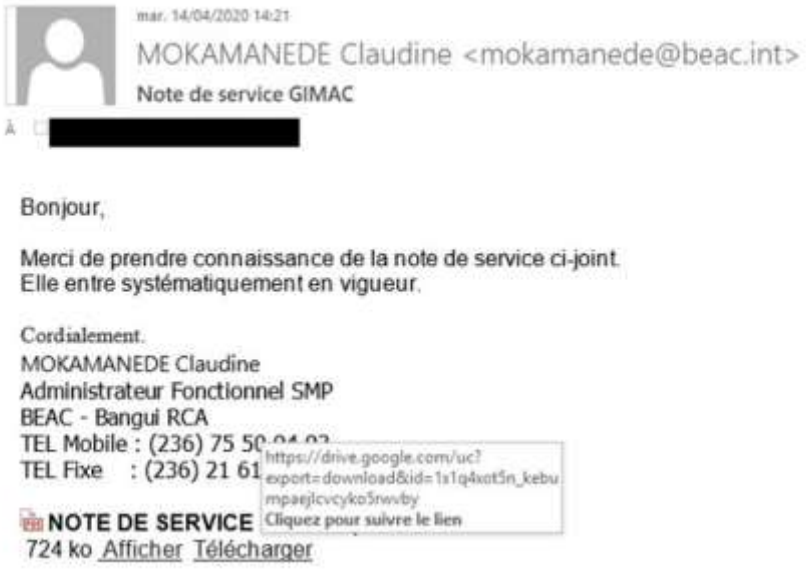
Group-IB и Orange CERT-CC публикуют свои результаты, включая TTP и индикаторы компрометации, чтобы помочь организациям, и особенно банкам, лучше выявлять атаки, связанные с этой группой. Они говорят, что ряд других исследователей безопасности помогли отследить группу, в том числе польский эксперт по разведке киберугроз Пшемыслав Сковрон, а также исследователи из Бельгии, Франции и Швейцарии, а также российский хостинг-провайдер Internet Hosting Center.

Они сообщают, что планы по подробному описанию деятельности группы в прошлом году были приостановлены после того, как злоумышленники заметили, что за ними следят, и немедленно удалили ряд учетных записей и изменили свою тактику, методы и процедуры.

«Когда это произошло, мы рисковали упустить их из виду», — говорит Рустам Миркасымов, руководитель отдела исследований киберугроз Group-IB в Европе, в своем блоге. «Чтобы не быть обманутыми, команда Group-IB отложила публикацию наших выводов до тех пор, пока они не раскроются снова».

Тем временем банда поразила еще как минимум пять целей, в том числе банки в Буркина-Фасо и Бенине в прошлом году, за которыми в этом году последовали два банка в Кот-д'Ивуаре и один в Сенегале.

Деятельность банды была впервые замечена в 2019 году, когда Orange CERT-CC «обнаружил масштабную фишинговую кампанию, нацеленную на банки и финансовые организации в Африке, и попросил помочь справиться с рядом инцидентов ИТ-безопасности для организации в Африке, которая сообщила о подозрительных банковских транзакциях. в выходные», — говорится в сообщении. «В ходе расследования аналитики безопасности быстро подтвердили аномальные транзакции, которые привели к снятию денег с банкоматов. Аналитики связали эту атаку с тем же субъектом, который был ответственен за фишинговую кампанию, и восстановили хронологию инцидента».



Фишинговая электронная почта, используемая группой, которая содержит ссылку на Google Диск, которая использовалась для доставки полезной нагрузки вредоносного ПО на компьютер жертвы. (Источник: Group-IB)

Исследователи говорят, что после получения доступа к сети жертвы злоумышленники остаются в сети от трех до 12 месяцев, прежде чем мошенническим образом снять средства с банкоматов. Злоумышленники, похоже, не имеют ничего уникального в своем арсенале для атак, а скорее используют свободно доступные инструменты, включая программное обеспечение с открытым исходным кодом и программное обеспечение, распространяемое через подпольные форумы по киберпреступности.

Похоже, что бандой руководят исключительно люди, для которых французский язык является основным. «Их английский довольно плохой, как и их русский», — говорится в отчете.

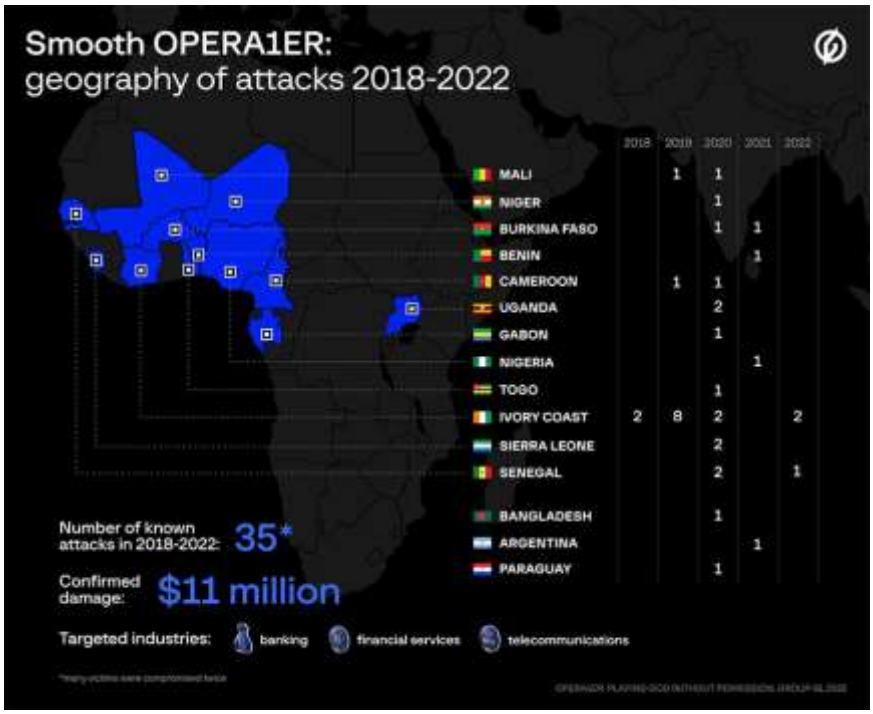
Исследователи говорят, что группа часто обналичивает свои атаки, используя денежные мулы для снятия наличных с мошеннических счетов, созданных злоумышленниками, через банкоматы. В одной атаке, как утверждается, использовалась «обширная сеть из 400 учетных записей мулов для мошеннического снятия денег».

Group-IB заявляет, что банда была впервые идентифицирована отчасти из-за того, что она использовала программное обеспечение Cobalt Strike для красной команды, в том числе развертывание маяков Cobalt Strike и настройку их для прослушивания порта 777. Хотя Cobalt Strike является коммерческим программным обеспечением, продаваемым как симуляции и операции красной команды», злоумышленники регулярно используют взломанные копии для распространения маяков Cobalt Strike — полезной нагрузки, которая устанавливается в системе — для заражения ПК и создания ботнетов, которыми они могут управлять с командно-контрольного сервера (см. Блокировать это). Теперь: Cobalt Strike и другие инструменты Red-Team).

Другие TTP, используемые бандой, которые, по словам исследователей, банкам следует остерегаться, включают использование BitRAT, трояна удаленного доступа, предназначенного для обхода средств защиты; развертывание собственной инфраструктуры VPN, такой как готовый FrootVPN, чтобы скрыть свою инфраструктуру; и использование бесплатных динамических DNS-сервисов, таких как DynDNS, часто в сочетании с диапазонами IP-адресов мобильного интернета в Кот-д'Ивуаре.

В ходе некоторых атак банда успешно получила доступ к программному обеспечению SWIFT — по всей видимости, приложению Alliance Access — которое использовалось банком. «В одном случае хакеры получили доступ к SMS-серверу, который можно было использовать для обхода антифрод или для обналичивания денег через платежные системы или системы мобильного банкинга», — говорится в сообщении. «В другом инциденте Opera1er использовала сервер обновлений антивируса, который был развернут в инфраструктуре в качестве точки опоры».

Исследователи говорят, что неясно, использовали ли злоумышленники свой доступ к программному обеспечению SWIFT для кражи средств, хотя это возможно. В некоторых случаях они также похищали средства после получения прямого доступа к платежным системам банка.



Источник: Group-IB». ***(Mathew J. Schwartz. Smooth 'Opera1er': French-Speaking Gang Steals $11 Million // Information Security Media Group, Corp. (https://www.govinfosecurity.com/smooth-opera1er-french-speaking-gang-steals-11-million-a-20400). 03.11.2022).***

***

«Агентство Европейского Союза по кибербезопасности (ENISA) определило и оценило 10 основных угроз кибербезопасности, которые возникнут к 2030 году, после проведения 8-месячного прогнозирования.

10 самых новых угроз кибербезопасности по версии ENISA:

Компрометация цепочки поставок программных зависимостей

Расширенные кампании по дезинформации

Рост авторитаризма цифрового наблюдения / потеря конфиденциальности

Человеческая ошибка и эксплуатируемые устаревшие системы в киберфизических экосистемах

Целевые атаки, усиленные данными смарт-устройств

Отсутствие анализа и контроля космической инфраструктуры и объектов

Рост передовых гибридных угроз

Нехватка навыков

Международные поставщики услуг ИКТ как единая точка отказа

Злоупотребление искусственным интеллектом

При поддержке группы экспертов ENISA по прогнозированию, сети CSIRT и экспертов EU CyCLOne ENISA провела семинар по выявлению угроз, чтобы найти решения возникающих проблем на горизонте 2030 года.

Исполнительный директор ENISA Юхан Лепассаар заявил: «Снижение будущих рисков невозможно ни отложить, ни избежать. Вот почему любой взгляд в будущее — наш лучший страховой план. Как говорится: «Профилактика лучше, чем лечение». Мы обязаны заранее принять все возможные меры, чтобы с годами повысить нашу устойчивость для улучшения ландшафта кибербезопасности в 2030 году и далее».

Упражнение показывает, что выявленные и классифицированные угрозы чрезвычайно разнообразны и включают наиболее актуальные на сегодняшний день. Тем не менее, ENISA заявляет, что сегодняшние угрозы еще предстоит устранить, поскольку их характер изменился. Агентство также отметило, что рост зависимости и популяризация новых технологий являются важными факторами, способствующими изменениям. Такие факторы усложняют упражнение и, таким образом, делают понимание угроз еще более сложным.

Методология ENISA, проводившаяся в период с марта по август 2022 года, включала совместные исследования, основанные на анализе политических, экономических, социальных и технологических факторов, также известных как анализ PESTLE, семинары по выявлению угроз и установлению их приоритетности.

В исследовании рассматривались четыре группы субъектов угроз, упомянутых в отчете ENISA Threat Landscape, и использовалась текущая таксономия угроз, разделяющая угрозы на категории высокого уровня с особым акцентом на преднамеренных угрозах.

Для выявления угроз специалисты, участвующие в проекте, прибегли к научно-фантастическому прототипированию или SFP.SFP состоит из историй, позволяющих участникам исследовать различные варианты будущего с разных точек зрения. SFP основан на сценарии будущего, основанном на тенденциях и переживаемом с точки зрения вымышленного персонажа…» ***(Supply Chain Compromise and Disinformation Rank High in EU's Top 10 Cyber Threats // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/supply-chain-compromise-and-disinformation-rank-high-in-eus-top-10-cyber-threats/). 14.11.2022).***

***

«Подавляющее большинство киберпреступлений в мире направлено на англоязычные страны, особенно на предприятия в США. Но есть признаки того, что крупные организованные группы активно прощупывают и занимают прибыльные ниши в других областях, проникая на территорию, на которую ранее охотились более мелкие и менее опытные злоумышленники. Группа безопасности Group-IB недавно опубликовала подробный отчет об одном таком примере, в котором описывается деятельность APT-группы «OPERA1ER» за последние несколько лет. Эта группа известна целевыми фишинговыми электронными письмами, но уникальна тем, что нацелена на менее развитые в экономическом отношении страны Африки, Азии и Латинской Америки.

Группа APT фокусируется на небольших франкоязычных экономиках, десятки атак, начиная с 2018 г.

Основываясь на том факте, что ее сообщения обычно на французском языке, и выбранной цели, считается, что группа APT действует из Африки. Однако его было трудно определить, несмотря на то, что он работает с 2018 года и за некоторые из этих лет было совершено более десятка успешных атак.

Эта APT-группа несет ответственность за 35 известных атак на общую сумму подтвержденного ущерба не менее 11 миллионов долларов. Group-IB считает, что реальная сумма может достигать $30 млн. Группа в основном ориентируется на африканские страны и отдает предпочтение предприятиям в сфере финансовых услуг, банковского дела и телекоммуникаций. Тем не менее, он не боится время от времени выходить из этой зоны комфорта. Группа также преследует компании в Бангладеш, Парагвае и Аргентине с помощью целевых фишинговых кампаний.

Еще одна особенность группы APT заключается в том, что она, похоже, использует исключительно готовые инструменты, а не разрабатывает собственные вредоносные программы или программы-вымогатели, как это делают крупнейшие преступные группировки. Необычно, чтобы группа, которая не разрабатывает свои собственные инструменты, просуществовала так долго или была так финансово успешна, и часть этого успеха, вероятно, связана с разумным выбором целей в областях, которые не сталкиваются с таким количеством ежедневных попыток, как в мире. крупнейшие экономики.

Еще одним ключом к его успеху является большая сеть счетов «денежных мулов», развернутых для снятия средств и направления средств в группу APT, которая, по сообщениям, насчитывает не менее 400 человек. Их метод целевого фишинга также описывается как «высококачественный» и точно воссоздает официальные правительственные уведомления и сообщения от крупных банков.

Группа APT также достаточно продвинута, чтобы замечать, когда охотники за угрозами следуют за ними по пятам. После четырех забастовок в 2021 году группа, похоже, заметила, что исследователи Group-IB отслеживали их и временно скрыли их операции, изменив некоторые TTP и удалив некоторые учетные записи, чтобы отвлечься от преследования. После нескольких месяцев бездействия группа вновь появилась в 2022 году, чтобы провести еще три своих характерных целевых фишинговых атаки по всей Африке.

«Изощренный» целевой фишинг нацелен на организации, которые не могут быть использованы для привлечения внимания группы APT.

Хотя его атаки были отслежены до 2018 года, Group-IB отмечает, что группа APT зарегистрировала свой первый известный домен в 2016 году. атаки, а в некоторых случаях группа до развертывания домена проходит до года.

Это может быть не то, что группы безопасности для организаций в некоторых из этих стран привыкли видеть среди обычных профилей угроз. Группа APT также парадоксально более сложна из-за того, что она использует только «готовое» вредоносное ПО, поскольку ей приходится придумывать творческие способы его развертывания, чтобы избежать обнаружения.

Целевые фишинговые кампании показывают, что группа также исследует ключевые фигуры в организациях, на которые они нацелены, а также защитные возможности; Group-IB отмечает, что это указывает на то, что злоумышленники либо подкупают инсайдеров, либо медленно и осторожно проникают в сети и проводят существенную разведку, прежде чем отправлять эти целевые фишинговые электронные письма, поскольку их подходы и побеги указывают на то, что они обладают закрытыми знаниями о своих жертвах.

Они также, кажется, точно знают, где находится больше всего денег, когда проникают в целевые организации, и выводят их, используя взломанные банковские компьютеры, которые имеют доступ к международному интерфейсу обмена банковскими сообщениями SWIFT. «Денежные мулы», которые фактически обналичивают выручку в банкоматах, набираются за несколько месяцев до атак. Кэшауты также проводятся в праздничные и выходные дни, чтобы воспользоваться ожидаемыми задержками времени ответа.

Хотя группа была привязана к какой-то части Африки, ее фактическое местонахождение до сих пор неизвестно после многих лет целевого фишинга, равно как и ее общий размер. В отчете говорится, что группа редко общается на английском или русском языках, а когда и общается, то плохо говорит на обоих языках. Group-IB отмечает, что группа APT обычно использует взломанную версию маяков Cobalt Strike вместе с трояном BitRAT и скрывает свою активность с помощью FrootVPN и бесплатных динамических DNS-сервисов, таких как DynDNS». ***(Scott Ikeda. APT Group Pilfers $11 Million From Africa, Asia, Latin America Using Spear Phishing Emails // CPO Magazine (https://www.cpomagazine.com/cyber-security/apt-group-pilfers-11-million-from-africa-asia-latin-america-using-spear-phishing-emails/). 15.11.2022).***

***

«Мошенничество с активным вымогательством нацелено на владельцев и администраторов веб-сайтов по всему миру, утверждающих, что они взломали их серверы, и требующих 2500 долларов США за предотвращение утечки данных.

Злоумышленники (самопрозванные Team Montesano) рассылают электронные письма с темами «Ваш веб-сайт, базы данных и электронные письма были взломаны».

Электронные письма, похоже, не являются целевыми, получатели требуют выкупа из всех вертикалей, включая личных блоггеров, правительственные учреждения и крупные корпорации.

Мошенничество настолько распространено, что наш собственный репортер Акс Шарма и создатель Have I Been Pwned Трой Хант также получили эти попытки вымогательства.

Спам-сообщения предупреждают, что хакеры утекут украденные данные, нанесут ущерб своей репутации и занесут сайт в черный список за спам, если жертвы не заплатят 2500 долларов.

FORWARD THIS EMAIL TO THE PERSON WITHIN YOUR COMPANY WHO MAKES THE IMPORTANT DECISIONS

You may have noticed that we are using your company's server to send this message, we have hacked into your https://www.axsharma.com site and extracted all of your databases and backed up all of your mailboxes.

How did this happen?

Our team found several vulnerabilities within your website and company computers that we were able to exploit. After finding them, we were able to obtain their database credentials and extract their complete data from their computers, from their site and copies of all emails in all their mailboxes with axsharma.com domain and finally we moved the information to a foreign server.

What does this mean?

We will systematically go through a series of steps to totally damage your reputation. First, your database will be leaked or sold to the highest bidder to be used for any purpose. Next, emails will be sent to all your customers, suppliers and business partners, stating that all of their information has been sold or leaked and your https://www.axsharma.com site was at fault for leaking the information and damaging the reputation of all your customers and providers. Lastly, any links you have indexed in search engines will be de-indexed based on the blackhat techniques we used in the past to de-index our targets, not to mention getting your business on every blacklist in the country.

How do I stop this?

We are willing to forget about destroying the reputation of your site and company for a small fee. The current fee is $2,500 USD in Bitcoins.

Электронное письмо с вымогательством репутации веб-сайта (Axe Sharma)

Полное сообщение о вымогательстве можно прочитать ниже:

ПЕРЕСЫЛИТЕ ЭТО ПИСЬМО СОТРУДНИКУ В ВАШЕЙ КОМПАНИИ, КОТОРЫЙ ПРИНИМАЕТ ВАЖНЫЕ РЕШЕНИЯ

Возможно, вы заметили, что мы используем сервер вашей компании для отправки этого сообщения, мы взломали ваш сайт https://www.***.gov и извлекли все ваши базы данных и создали резервные копии всех ваших почтовых ящиков.

Как это случилось?

Наша команда обнаружила несколько уязвимостей на вашем веб-сайте и компьютерах компании, которые мы смогли использовать. Найдя их, мы смогли получить их учетные данные из базы данных и извлечь их полные данные с их компьютеров, с их сайта и копии всех электронных писем во всех их почтовых ящиках с доменом ***.gov, и, наконец, мы переместили информацию на чужой сервер..

Что это значит?

Мы будем систематически предпринимать ряд шагов, чтобы полностью повредить вашей репутации. Во-первых, ваша база данных будет украдена или продана тому, кто предложит самую высокую цену, для использования в любых целях. Затем всем вашим клиентам, поставщикам и деловым партнерам будут разосланы электронные письма с сообщением о том, что вся их информация была продана или просочилась, а ваш сайт https://***.gov был виновен в утечке информации и подрыве репутации. всех ваших клиентов и поставщиков. Наконец, любые ссылки, которые вы проиндексировали в поисковых системах, будут удалены из индекса на основе методов черных шляп, которые мы использовали в прошлом

для деиндексации наших целей, не говоря уже о том, что ваш бизнес попал во все черные списки в стране.

Как мне остановить это?

Мы готовы забыть об разрушении репутации вашего сайта и компании за небольшую плату. Текущая комиссия составляет 2500 долларов США в биткойнах.

Отправьте сумму в биткойнах по следующему адресу:

3Fyjqj5WutzSVJ8DnKrLgZFEAxVz6Pddn7

Как только вы произведете оплату, мы автоматически сообщим об этом. В тот момент, когда вы прочитали это сообщение, у вас есть 72 часа, чтобы произвести платеж, или я гарантирую, что репутация вашей компании будет полностью уничтожена. Доказательством того, что у нас есть доступ и все ваши данные, является то, что это сообщение было отправлено с использованием серверов вашей компании.

Как получить биткойны?

Вы можете легко купить биткойны через различные веб-сайты.

Что произойдет, если я не заплачу?

Если вы решите не платить, мы запустим атаку через 72 часа и будем держать ее до тех пор, пока вы этого не сделаете, противодействия этому нет, вы просто потратите больше денег, пытаясь найти решение. Мы полностью разрушим вашу репутацию среди ваших клиентов, ваших поставщиков, ваших партнеров, в Google и во всей стране.

Это не обман, не пытайтесь рассуждать или договариваться, мы не будем читать никаких ответов. Как только вы заплатите, мы прекратим то, что мы делали, мы уничтожим все данные, взятые с вашего сайта, ваших баз данных, ваших почтовых ящиков, и вы больше никогда о нас не услышите.

Имейте в виду, что платеж с помощью биткойнов является анонимным, и никто не узнает, что вы его выполнили. Время бежит.

Судя по электронным письмам с вымогательством, увиденным BleepingComputer, злоумышленники в настоящее время используют два биткойн-адреса.

3Fyjqj5WutzSVJ8DnKrLgZFEAxVz6Pddn7

3PmYSqtG5x5bGNrsYUy5DGtu93qNtsaPRH

К сожалению, транзакции биткойнов на кошелек 3Fyjqj5WutzSVJ8DnKrLgZFEAxVz6Pddn7 указывают на то, что кто-то, возможно, уже оплатил требование о вымогательстве.

Несмотря на то, что эти электронные письма могут пугать тех владельцев веб-сайтов, которые их получают, важно помнить, что это всего лишь мошенничество.

Они массово рассылаются по электронной почте многим людям и просто пытаются напугать людей, чтобы они совершили платеж. Вместо этого просто отметьте их как спам и удалите.

Кроме того, всегда ищите биткойн-адрес, встроенный в электронное письмо с шантажом, которое вы получаете, в базе данных о злоупотреблениях биткойнами, чтобы найти любые сообщения о мошенниках, активно использующих их…». ***(Sergiu Gatlan. New extortion scam threatens to damage sites' reputation, leak data //***

Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-extortion-scam-threatens-to-damage-sites-reputation-leak-data/). 12.11.2022).

***

«Ажиотаж и популярность чемпионата мира по футболу привлекли зрителей со всего мира. А это, в свою очередь, привлекает различных киберпреступников, которые хотят использовать многочисленных фанатов и участвующие организации, чтобы быстро заработать.

Кампании с продвинутыми постоянными угрозами (APT), фишинг, мошенничество с кредитными картами и криптовалютами, DDoS-атаки и кража личных данных входят в число угроз, с которыми сталкиваются организации и аудитория, сообщает CloudSEK. Киберпреступники мотивированы финансовой выгодой, идеологией или геополитической принадлежностью.

Объяснение кибератак на тему чемпионата мира по футболу

Обналичивание украденных кредитных карт: Кардинговые группы продают данные украденных кредитных карт для проведения незаконных и несанкционированных транзакций. Они также предоставляют услуги по обналичиванию денег с этих карт, используя предоплаченные подарочные карты, чтобы замести следы. Кардинговые группы могут использовать поддельные сайты на тему FIFA, чтобы собирать данные карт у ничего не подозревающих пользователей, а затем использовать их для бронирования отелей и авиабилетов.

Продажа поддельных карт Hayya: Из-за важности карт Hayya (разрешение на въезд ФИФА) во время чемпионата мира злоумышленники продают поддельные карты Hayya ничего не подозревающим болельщикам, которые готовы заплатить любую сумму, чтобы получить ее.

Было обнаружено, что несколько каналов Telegram продают карты Hayya по цене от 50 до 150 долларов. Злоумышленники утверждают, что для создания карт Hayya требуются действительные удостоверения личности покупателя, такие как паспорта. И оплата принимается только в биткойнах.

Поддельные карты Hayya. Злоумышленники также делятся методами взлома, которые якобы позволяют бесплатно зарегистрировать карту Hayya без действительного номера билета FIFA. Этот метод основан на подборе номера тикета на основе предполагаемого шаблона номера тикета, которым поделился злоумышленник: «300 и 4 случайные цифры».

Поддельные крипто-токены и монеты. Учитывая, что Crypto.com является официальным спонсором FIFA, а Binance сотрудничает с Кристиано Роналду для продвижения NFT на футбольную тематику, злоумышленники используют эту шумиху, чтобы продавать поддельные «монеты чемпионата мира» и « World Cup Token», продвигая их как криптовалюту с ограниченным тиражом. Однако большинство из этих предполагаемых монет не существует.

Мошенничество с фишингом и продажей билетов. Поскольку чемпионат мира по футболу является популярным событием, спрос на билеты намного превышает предложение. Чтобы воспользоваться этим разрывом между спросом и предложением, мошенники создали веб-сайты, продающие поддельные билеты.

DDoS-атаки. Злоумышленники и хактивисты утверждают, что запускали DDoS-атаки на базирующиеся в Катаре организации, такие как qatargas.com и moci.gov.qa. Они также поделились доказательством того, что сайты, на которые они нацелены, отключены из-за их атак.

Услуги по ставкам и азартным играм. Как и в случае с выборами или другими спортивными событиями, азартные игры и ставки на исход матчей чемпионата мира по футболу являются обычным явлением. Злоумышленники используют это, чтобы делиться советами по прогнозированию за определенную цену, продвигать поддельные сайты ставок, которые крадут деньги пользователей и персональные данные, а также распространяют приложения для азартных игр, пронизанные вредоносным ПО.

«Разрыв между спросом и предложением билетов на матчи чемпионата мира по футболу, авиабилетов, отелей, сувениров и т. д. был использован киберпреступниками для обмана болельщиков и энтузиастов. Несмотря на привлекательные предложения и приманки, пользователям следует ограничить свои покупки официальными сайтами и мобильными приложениями. А компании, являющиеся спонсорами FIFA, должны укреплять свои механизмы безопасности и быть в курсе тактики и методов злоумышленников», — сказал исследователь CloudSEK.

Рекомендации для болельщиков FIFA

Покупайте билеты FIFA и карты Hayya только на официальном сайте.

Подтвердите легитимность криптовалют, прежде чем инвестировать в них.

Не пользуйтесь услугами, связанными с FIFA, в Telegram или социальных сетях.

Не сообщайте свою личную информацию или банковские реквизиты неизвестным лицам или веб-сайтам.

Не устанавливайте приложения, опубликованные через Telegram, социальные сети или сторонние магазины приложений.

Просмотрите разрешения, запрашиваемые приложениями, и отключите разрешения, которые не нужны для работы приложения.

Будьте осторожны со схемами, которые кажутся слишком хорошими, чтобы быть правдой.

Рекомендации для участвующих организаций

Балансировщики нагрузки пользователей или сервисы, такие как Cloudflare, чтобы избежать DDoS-атак.

Используйте брандмауэр и обновляйте программное обеспечение до последней версии.

Проводите информационные кампании, чтобы информировать поклонников и пользователей о законных порталах и веб-сайтах.

Мониторинг в режиме реального времени и удаление фишинговых сайтов, поддельных приложений и подражательных страниц в социальных сетях…». ***(Cybercriminals are cashing in on FIFA World Cup-themed cyberattacks // Help Net Security (https://www.helpnetsecurity.com/2022/11/29/fifa-world-cup-themed-cyberattacks/). 29.11.2022).***

***

«Хакери зламали безліч компаній із Росії й вимагали викуп за вкрадені корпоративні дані. Про це пише російський сайт CNews, посилаючись на аналітичну фірму BI.ZONE, що спеціалізується на цифрових ризиках.

З серпня 2022 року хакери зламали десятки компаній, переважно з малого та середнього бізнесу, скориставшись вразливістю сервісу корпоративної пошти Microsoft Exchange. Як заявили в BI.ZONE, зловмисники скористалися спеціальною програмою, яка проникла на поштовий сервер та дозволила звантажити всі листи разом із прикріпленими до них файлами.

Як пояснив директор департаменту моніторингу, реагування та дослідження кіберзагроз BI.ZONE Теймур Хеірхабаров, вразливість Microsoft Exchange розкрили ще восени минулого року, і розробники швидко її усунули. Жертвами зламів стали російські підприємства, які не встановили оновлення на сервер.

Компанії не помічали злому і не знали про витік даних доти, доки кіберзлочинці не почали відправляти фахівцям з безпеки повідомлення з електронної адреси security4real@proton.me. Вони зловмисники пропонували сплатити послуги "аудиту безпеки" в обмін на повернення баз даних, а фактично вимагали заплатити викуп, і в деяких випадках — до $10 тис.

Дослідники з Positive Technologies підрахували, що в першій половині 2022 кількість атак на російські компанії зросла на 18% в порівнянні з попереднім півріччям. Підприємства малого бізнесу рідше страждають від кіберзлочинів, ніж середній та великий. Хакери часто використовують уразливості у мережному обладнанні компаній, виявляючи їх шляхом масового сканування. У них підготовлені скрипти, які виконують атаки в автоматичному режимі, як тільки перебуває пролом у захисті.

Великою популярністю користуються методи соціальної інженерії, такі як фішинг. З їх допомогою хакери одержують облікові дані або іншу конфіденційну інформацію. Наприклад, жертвам розсилають листи з прикріпленими «вірусами», які допомагають красти дані, шифрують файли або ж потай використовують комп'ютери для майнінгу криптовалюти». ***(Хакери зламали десятки російських компаній і вимагають викупу: як їм це вдалося // Internetua (https://internetua.com/hakeri-zlamali-desyatki-rosiiskih-kompanii-i-vimagauat-vikupu-yak-yim-ce-vdalosya). 22.11.2022).***

***

«…В Южной Африке ряд организаций и ведомств, связанных с правительством, попали в число тех, кто подвергся атакам, при этом один громкий инцидент привел к нарушению работы на две недели, что привело к убыткам на сумму до 1 миллиарда рандов.

Но в то время как атаки на критическую инфраструктуру вызывают серьезные сбои, которые попадают в заголовки, атаки на важнейшие системы в ведомствах государственного сектора — вплоть до местных муниципалитетов — могут быть в равной степени разрушительными и разрушительными для пострадавших. Ранее в этом месяце в результате нападения на небольшой местный муниципалитет на несколько дней были отключены его системы, электронная почта и стационарные телефоны.

Государственный сектор должен не только поддерживать операционную устойчивость; он также должен защищать и защищать личные и конфиденциальные данные своих граждан, снижать риск мошенничества и кражи государственных средств, а также обеспечивать контроль производительности и затрат в рамках своих усилий по снижению киберрисков.

Являясь предпочтительным поставщиком систем безопасности для государственного сектора Южной Африки, BCX работала со многими агентствами государственного сектора на местном, региональном и национальном уровнях, чтобы помочь им снизить киберриски. По нашему опыту, ИТ-директора и директора по информационной безопасности в государственном секторе хорошо осведомлены о растущем киберриске и прилагают все усилия для защиты своих организаций. Но при этом они сталкиваются с рядом проблем.

Ключевой вопрос заключается в том, что устаревшие системы все еще широко используются во многих учреждениях государственного сектора. Поскольку некоторым системам уже более 40 лет и они больше не поддерживаются, эти системы являются потенциальными точками входа, которые делают уязвимыми всю их экосистему. Департаменты изо всех сил пытаются интегрировать эти устаревшие системы и имеют ограниченный доступ к ним. Эти системы часто также зависят от ручных процессов, которые подвергают эти отделы дополнительным рискам мошенничества и человеческих ошибок.

Безопасность также подвергается угрозе из-за все более сложных сред, включающих несколько разрозненных решений безопасности, которые со временем добавляются для устранения различных аспектов риска. Без стратегического проектирования, интеграции и прозрачности среды эти системы не будут давать оптимальных результатов и могут даже затруднить снижение рисков.

Еще одной проблемой является постоянная нехватка навыков кибербезопасности. Департаменты государственного сектора, как и их коллеги из частного сектора, сталкиваются с трудностями при наборе и сохранении высококвалифицированных специалистов в области кибербезопасности, необходимых для того, чтобы опережать постоянно меняющуюся киберпреступность.

Многим отделам также сложно правильно понять самые основы кибербезопасности: у них могут быть решения, которые не были обновлены в соответствии с последними приемлемыми стандартами, используемые устройства

могут быть небезопасными, а конечные пользователи могут быть не в курсе последних событий. тактики и риски киберпреступлений.

Для решения этих задач по снижению риска требуется целостный подход, обычно реализуемый поэтапно. Как системный интегратор, мы располагаем хорошими возможностями для внедрения комплексных решений, которые комплексно снижают риски.

Не существует серебряной пули, которая мгновенно защитит такие организации. Разработка эффективных решений требует консультативного подхода, когда мы понимаем их текущий уровень зрелости, используем упреждающие оценки для выявления уязвимостей, устраняем слабые места для быстрых побед и разрабатываем устойчивый план для улучшения профиля рисков организации с течением времени.

Важные меры по снижению риска также включают внедрение стратегий нулевого доверия, мониторинг и оценку, а также создание Оперативного центра безопасности». ***(Sinamava Hina-Mvoko. Public sector must reimagine cyber security to enable e-government ideal // Daily Maverick (https://www.dailymaverick.co.za/article/2022-11-07-public-sector-must-reimagine-cyber-security-to-enable-e-government-ideal/). 07.11.2022).***

***

«В то время как потребители могут искать мошеннических розничных продавцов, поскольку кризис стоимости жизни углубляется, киберпреступники также неистовствуют в этом секторе с целым рядом автоматических угроз — от захвата учетной записи, мошенничества с кредитными картами, веб-скрапинга, злоупотреблений API, ботов Grinch. и распределенные атаки типа «отказ в обслуживании» (DDoS) — все это становится постоянной проблемой для индустрии электронной коммерции, угрожая онлайн-продажам и удовлетворенности клиентов.

Продолжающийся шквал атак на веб-сайты, приложения и API-интерфейсы ритейлеров в течение календарного года и в разгар сезона праздничных покупок представляет собой постоянный бизнес-риск для отрасли розничной торговли, говорится в последнем отчете «Состояние безопасности в электронной коммерции 2022». Имперва.

«Сезон праздничных покупок — критический период для розничной торговли, и угрозы безопасности могут снова подорвать прибыль ритейлеров в 2022 году, — говорит Линн Маркс, старший менеджер по продуктам Imperva. «Эта отрасль сталкивается с множеством угроз безопасности, большинство из которых автоматизированы и действуют круглосуточно. Ритейлерам нужен единый подход, чтобы остановить эти постоянные атаки, ориентированный на защиту данных и способный быстро смягчить атаки, не мешая покупателям».

Автоматизированный противник: плохие боты и онлайн-мошенничество преследуют розничные сайты

За последние 12 месяцев почти 40% трафика на сайтах ритейлеров исходило не от людей. Вместо этого он исходил от бота, программного приложения, контролируемого операторами, которые запускают автоматизированные задачи,

часто со злым умыслом. В сфере розничной торговли печально известный бот Grinch известен тем, что накапливает запасы во время сезона праздничных покупок, собирая товары с высоким спросом и затрудняя покупателям покупку подарков в Интернете.

Из всего трафика на веб-сайтах ритейлеров почти четверть (23,7%) была связана именно с плохими ботами, вредоносными автоматами, которые способствуют онлайн-мошенничеству. Доля продвинутых ботов — скриптов, которые используют новейшие методы уклонения, чтобы имитировать поведение человека и избежать обнаружения — на розничных сайтах выросла по сравнению с предыдущим годом (с 23,4% до 31,1%). Усовершенствованные боты представляют собой серьезную проблему для организаций, чтобы остановить их без надлежащей защиты.

В 2021 году количество атак, связанных с ботами, на сайты розничной торговли выросло на 10% в октябре и выросло еще на 34% в ноябре, что говорит о том, что операторы ботов активизируют свои гнусные действия в пиковые периоды праздничных покупок.

Захват учетной записи (ATO) — это еще одна форма онлайн-мошенничества, при которой киберпреступники пытаются скомпрометировать онлайн-аккаунты, используя украденные пароли и имена пользователей. В 2021 году в 64,1% атак ATO использовался продвинутый плохой бот. Из всех попыток входа на веб-сайты розничной торговли 22,6% были вредоносными, что почти в два раза больше, чем на сайтах других отраслей. Злоумышленники использовали украденные учетные данные в 94,7% случаев в атаках с заполнением учетных данных, нацеленных на розничных продавцов, по сравнению с 69,6% времени в других отраслях.

Злоупотребления API и атаки множатся, создавая новые проблемы для ритейлеров

API — это невидимая соединительная ткань, которая позволяет приложениям обмениваться данными и вызывать цифровые сервисы. Анализ, проведенный Imperva Threat Research, показывает, что на трафик через API приходится 41,6% всего трафика на сайты и приложения интернет-магазинов.

Из них 12% трафика направляется на конечные точки, такие как базы данных, где хранятся личные данные (учетные данные, идентификационные номера и т. д.). Более того, от 3 до 5% трафика API направляется на недокументированные или теневые API, конечные точки, о существовании которых специалисты по безопасности не знают или которые больше не защищают.

Открытые или уязвимые API-интерфейсы представляют серьезную угрозу для розничных продавцов, поскольку злоумышленники могут использовать API в качестве пути для кражи данных клиентов и платежной информации. Злоупотребления API часто осуществляются посредством автоматических атак, когда ботнет заливает API нежелательным трафиком в поисках уязвимых приложений и незащищенных данных.

В 2021 году количество атак API увеличилось на 35% в период с сентября по октябрь, а затем увеличилось еще на 22% в ноябре, помимо повышенного уровня атак в предыдущие месяцы. Этот вывод свидетельствует о том, что злоумышленники масштабируют свои усилия в сезон праздничных покупок, поскольку между API-

интерфейсами и приложениями, обеспечивающими работу сервисов электронной коммерции, происходит обмен большим объемом данных.

Остерегайтесь простоев: ddos-атаки продолжают угрожать ритейлерам

Распределенная атака типа «отказ в обслуживании» (DDoS) — это автоматизированная угроза, которая пытается нарушить критически важные бизнес-операции, переполняя сеть или инфраструктуру приложений вредоносным трафиком. Атаки часто запускаются ботнетом, группой скомпрометированных подключенных устройств, которые распределены по Интернету и управляются одной стороной.

Imperva Threat Research считает, что DDoS-атаки в 2022 году будут более масштабными и сильными во всех отраслях. Количество зарегистрированных инцидентов со скоростью более 100 Гбит/с удвоилось, а количество атак со скоростью более 500 Гбит/с/0,5 Тбит/с увеличилось на 287%. Более того, те, на кого направлена атака, часто подвергаются повторной атаке в течение 24 часов. Imperva считает, что 55% веб-сайтов, пострадавших от DDoS-атак на уровне приложений, и 80%, пострадавших от DDoS-атак на сетевом уровне, подвергались многократным атакам.

DDoS-атака — постоянная угроза для ритейлеров. Простои, вызванные DDoS-атакой, могут привести к нарушению работы сайта, репутационному ущербу и потере доходов. DDoS представляет собой серьезную угрозу для интернет-магазинов, которые полагаются на производительность и доступность приложений для обеспечения работы цифровых витрин». ***(Paul Skeldon. 40% of traffic to ecommerce sites comes from bots raising cyber security threat level // InternetRetailing Media (https://internetretailing.net/technology/40-of-traffic-to-ecommerce-sites-comes-from-bots-raising-cyber-security-threat-level/). 09.11.2022).***

***

Діяльність хакерів та хакерські угруповування

«Компанія ESET, розробник популярного антивірусу, повідомила про поширення підроблених шкідливих VPN, які розповсюджують індійські хакери з угруповання Bahamut.

Найчастіше хакери підробляють відомі VPN-клієнти SecureVPN, SoftVPN та OpenVPN. При встановленні такої програми вірус таємно отримує доступ до SMS користувача, історії дзвінків, розташування пристрою та будь-якої іншої інформації. Про це розповів дослідник інформаційної безпеки ESET Лукаш Штефанко.

Особливість вірусу в тому, що з його допомогою хакери можуть зламати захищені подвійним шифруванням месенджери WhatsApp, Telegram або Signal. Тобто зловмисники можуть отримати доступ до всіх даних пристрою без відома жертви.

При цьому жодна з фейкових програм не поширюється через Google Play». ***(Хакери почали розповсюджувати підроблений VPN для злому месенджерів // Internetua (https://internetua.com/hakeri-pocsali-rozpovsuadjuvati-pidroblenii-vpn-dlya-zlomu-mesendjeriv). 26.11.2022).***

***

«Докладчик комитета PEGA Софи ин 't Вельд призывает к мораторию на шпионское ПО Акшая Асокан.

Член Европарламента обвинил Евросоюз в соучастии в распространении продвинутого шпионского ПО в государствах-членах и по всему миру.

Представляя во вторник предварительные выводы парламентского комитета, расследующего с марта злоупотребление шпионскими инструментами, такими как Pegasus, представитель Нидерландов Софи ин 't Вельд назвала приложения угрозой для демократии.

Исполнительный орган союза привык бороться с внешними угрозами демократии, «но когда угроза демократии исходит изнутри, Комиссия молчит», — заявил голландский член альянса либеральных представителей Renew Europe, имея в виду Европейскую комиссию.

Она добавила, что индустрия коммерческого передового шпионского ПО «полностью европеизирована, используя внутренний рынок, Шенген и репутацию лейбла ЕС». Группа анализа угроз Google сообщает, что она определила 30 мировых производителей наемнического шпионского ПО, из которых наиболее известна израильская NSO Group, производитель Pegasus. Вельд является докладчиком комитета, то есть она представит окончательный отчет. Шенген относится к территории 26 государств-членов, где пограничный контроль был отменен.

«Все государства-члены имеют в своем распоряжении шпионское ПО. Даже если они не признают этого, они это делают», — сказала она.

В марте Европейский парламент подавляющим большинством голосов проголосовал за назначение комитета PEGA из 38 членов после того, как появились сообщения о том, что власти Польши, Греции, Венгрии и Испании использовали Pegasus для слежки за политиками, журналистами и активистами. В наиболее продвинутом варианте Pegasus может заразить мобильное устройство без необходимости переходить по вредоносной ссылке. Целенаправленная слежка посредством незаметных заражений мобильных устройств — это всемирная проблема с политическими разветвлениями, которые ощущаются повсюду, от Мексики до Индии.

Кипр и Болгария действуют как экспортные центры для шпионского ПО и пользуются слабым соблюдением правил в отношении товаров двойного назначения, заявил Вельд.

«Люксембург — это место, где продавцы шпионского ПО ведут свой финансовый бизнес. Ирландия предлагает привлекательные фискальные условия. Интересно, что Мальта кажется удобным домом для боссов шпионского ПО с золотыми паспортами и компаниями, занимающимися почтовыми ящиками», — добавила она.

«Италия, Франция и Австрия являются домом для некоторых очень важных производителей и поставщиков шпионского ПО. В Чешской Республике каждый год проходит большая ярмарка шпионского ПО», — продолжила она.

В понедельник правительство Греции объявило о своем намерении запретить продажу шпионского ПО после того, как газета опубликовала список из более чем 30 человек, чьи смартфоны предположительно были заражены передовым шпионским ПО. В список вошли министры правительства и бизнесмены, сообщает Reuters.

Председатель комитета PEGA Йерун Ленарс пожаловался, что национальные правительства препятствуют расследованию, ссылаясь на беспочвенные соображения национальной безопасности, и Вельд повторил эти обвинения (см. Расследование Пегаса в Европейском парламенте сталкивается с сопротивлением).

«Они вытягивают карту национальной безопасности, и с этого момента дверь закрыта, окно закрыто, никаких вопросов, никакой ответственности, вы не получаете никакой информации», — сказала она.

Она предложила европейский мораторий на современные шпионские программы, который можно было бы снять в каждой стране только после демонстрации определенных условий, включая расследования злоупотреблений, правовую основу для приемлемого использования, позволяющую Европолу расследовать заявления о незаконном использовании, и отмену все экспортные лицензии не полностью соответствуют правилам в отношении товаров двойного назначения.

По словам Велда, пресечение передовых шпионских программ потребует наднациональных мер, задав вопрос, способен ли Европейский союз справиться с этой задачей. «Когда дело доходит до защиты самого главного, демократии и свободы, Европа слаба и бессильна».

В заявлении Ленарса после пресс-конференции Велда подчеркивается предварительный характер доклада. «Все члены комитета PEGA будут иметь возможность представить поправки к проекту отчета. Только окончательный отчет и рекомендации, принятые в конце периода нашей деятельности, представляют позицию Европейского парламента в целом», — сказал он. Сказал». ***(Akshaya Asokan. EU Complicit in Spread of Advanced Spyware, Charges Veld // Information Security Media Group, Corp. (https://www.govinfosecurity.com/eu-complicit-in-spread-advanced-spyware-charges-veld-a-20438). 08.11.2022).***

***

«…Согласно отчету CyberTheory за третий квартал 2022 года, активность вредоносных программ увеличилась на 28% по сравнению с прошлым годом, а активность ботнетов и эксплойтов выросла более чем на 100%. Директор CyberTheory Стив Кинг говорит, что для борьбы с сегодняшними киберпреступлениями необходим «новый подход к защите от кибербезопасности».

Кинг говорит, что лидеры службы безопасности должны сделать так, чтобы противникам было намного труднее преуспеть в их обороне. «Повышая контроль в рамках процесса управления идентификацией и доступом, удаляя избыточное

доверие из сети, изолируя наши корпоративные активы и защищая поверхности, мы сможем это сделать», — говорит он.

Кинг также советует сосредоточиться на видимости сети и подавлении вторжений. «Возможно, гораздо эффективнее просто наблюдать, как злоумышленники делают то, что они делают», — говорит Кинг. Эта разведывательная информация даст защитникам лучшее представление о «намерениях преступников, куда они направляются, а также даст нам более высокую и более эффективную скорость поимки», добавляет он…». ***(Anna Delaney. Why Today's Cyber Defense Requires Offensive Thinking // Information Security Media Group, Corp. (https://www.govinfosecurity.com/todays-cyber-defense-requires-offensive-thinking-a-20425). 08.11.2022).***

***

«В отчете Imperva «Состояние безопасности в электронной коммерции 2022» указано, что боты несут ответственность за большинство инцидентов с безопасностью, включая атаки с автоматическим захватом учетных записей на розничных продавцов электронной коммерции.

Согласно отчету, 40% трафика на розничных веб-сайтах исходит от ботов, запрограммированных на выполнение автоматических действий, обычно со злым умыслом. Впоследствии 62% атак на веб-сайты ритейлеров были совершены с помощью автоматических скриптов по сравнению с 28% атак в других отраслях. К ним относятся боты Grinch, накапливающие товары повышенного спроса, и вредоносные боты, часто выполняющие атаки на веб-сайты, приложения и API-интерфейсы розничных продавцов.

Imperva обнаружила, что атаки, начиная от захвата учетной записи, мошенничества с кредитными картами, веб-скрапинга, злоупотребления API, ботов Grinch и DDoS-атак, представляют собой серьезную проблему для розничных продавцов электронной коммерции, угрожая онлайн-продажам и удовлетворенности клиентов.

Бот-трафик угрожает интернет-магазинам

Хотя большая часть всего трафика на сайты и приложения интернет-магазинов по-прежнему приходилась людям, трафик ботов значительно увеличился за 12 месяцев.

В то время как трафик плохих ботов остался относительно неизменным на уровне 23,7%, количество хороших ботов увеличилось до 16,6%, в результате чего общий автоматизированный трафик достиг 40,3%.

Удивительно, но объем трафика вредоносных ботов на веб-сайтах интернет-магазинов был ниже среднего показателя в 30,7%, хотя уровень их сложности был выше среднего. За 12 месяцев присутствие продвинутых плохих ботов на розничных сайтах увеличилось с 23,4% до 31,1% по сравнению с общим средним показателем в 22,1%.

Хотя хорошие боты не причиняют вреда, исследователи предупреждают, что они по-прежнему представляют онлайн-угрозу, искажая аналитику и снижая показатели конверсии. Точно так же низкий трафик плохих ботов не указывает на

снижение рисков, поскольку сложные боты могут достигать своих целей с меньшим количеством запросов.

«Они часто выбирают «низкую и медленную» тактику, которая позволяет им проводить серьезные атаки с использованием меньшего количества запросов и даже задерживать запросы, что позволяет им не выделяться из обычных моделей трафика и избегать срабатывания порогов обнаружения безопасности на основе скорости», — говорится в отчете.

По словам исследователей, операторы ботов пошли на многое, чтобы замести следы, используя различные тактики уклонения. Например, они имитировали человеческое поведение и использовали механизмы анонимности, такие как анонимные прокси и TOR, чтобы избежать идентификации.

За период наблюдения объем анонимных атак увеличился с 3,5% до 33% в течение года. Таким образом, хотя объем трафика плохих ботов на розничных сайтах оставался постоянным в 2021 году, он был более разрушительным, и его было сложнее обнаружить и заблокировать, чем годом ранее.

Ритейлеры электронной коммерции чаще сталкиваются с атаками с захватом аккаунта

В атаках с захватом учетной записи (ATO) киберпреступники используют украденные пароли и имена пользователей для компрометации онлайн-аккаунтов. Эти атаки могут также включать создание поддельных учетных записей с использованием украденных учетных данных.

Согласно отчету Imperva о состоянии безопасности, атаки ATO непропорционально чаще нацелены на розничных продавцов электронной коммерции, чем на другие отрасли. Например, розничные продавцы электронной коммерции столкнулись с 22,6% злонамеренных попыток входа в учетную запись, что почти вдвое превышает средний показатель (11,6%). Злоумышленники также использовали украденные учетные данные в 94,7% атак с использованием учетных данных против розничных продавцов электронной коммерции по сравнению с 69,6% в других отраслях. Кроме того, в атаках с захватом учетных записей широко использовались сложные боты, при этом злоумышленники использовали продвинутых плохих ботов в 64,1% атак ATO.

Конечная цель атак с захватом учетных записей заключалась в краже сохраненной информации о кредитных картах, остатках на подарочных картах, бонусных баллах и других преимуществах для клиентов. По мнению исследователей, атаки с захватом учетных записей усиливаются во время курортного сезона или других глобальных событий, таких как война в Украине.

Распределенные атаки типа «отказ в обслуживании» (DDoS) активизировались в разных отраслях

Исследование угроз Imperva показало, что DDoS-атаки в 2022 году будут более масштабными и сильными во всех отраслях. Такие атаки исходят от группы скомпрометированных подключенных устройств через Интернет, управляемых одним злоумышленником.

Согласно Imperva, DDoS-атаки были постоянной и серьезной угрозой для розничных продавцов электронной коммерции, полагающихся на производительность и доступность приложений для онлайн-бизнеса.

Imperva обнаружила, что атаки со скоростью более 100 Гбит/с утроились, а атаки со скоростью более 500 Гбит/с увеличились на 287%. Кроме того, 55% всех приложений, пострадавших от DDoS-атак на уровне приложений, и 80% приложений, пострадавших от DDoS-атак на сетевом уровне, подвергались атакам несколько раз.

Imperva заявила, что простои, вызванные DDoS-атакой, могут привести к сбоям в работе, репутационному ущербу и потерям доходов для розничных продавцов электронной коммерции.

Злоупотребление API становится растущей проблемой

Интерфейсы прикладного программирования (API) — это «соединительная ткань», которая позволяет приложениям обмениваться данными, потреблять и предоставлять цифровые услуги. Таким образом, API были источником 42% онлайн-трафика на веб-сайтах розничных продавцов электронной коммерции.

Кроме того, 12% трафика API направляется на конечные точки с доступом к конфиденциальным личным данным, таким как учетные данные, идентификационные номера и т. д.

Было отмечено, что 3–5% трафика API направляется на теневые API, о существовании которых службы безопасности не знают и, следовательно, не могут их защитить. Впоследствии злоупотребления открытыми или теневыми API стали путями для кражи данных клиентов и платежной информации.

Imperva обнаружила, что злоупотребление API увеличилось на 35% в период с сентября по октябрь 2021 года, а затем снова увеличилось еще на 22% в ноябре, что превышает повышенный уровень атак в предыдущие месяцы. Эти наблюдения показали, что боты были более активны в разгар сезона праздничных покупок, и ситуация не изменится в 2022 году.

Imperva посоветовала ритейлерам электронной коммерции подготовиться к большому трафику и DDoS-атакам в разгар праздничного сезона и ожидать, что боты будут нацелены на их маркетинговые кампании. Другие рекомендации включают в себя защиту функций своего веб-сайта, инвентаризацию javascript и служб на стороне клиента, а также опережение мошенников, предупреждая клиентов о фишинговых атаках». ***(Alicia Hope. Europol Arrested a “High Value” Russian-Canadian LockBit Ransomware Operator for Extradition to the US // CPO Magazine (https://www.cpomagazine.com/cyber-security/62-of-security-incidents-on-ecommerce-retailers-originate-from-bots-including-account-takeover-ddos-and-api-attacks/). 11.11.2022).***

***

«Фирма по анализу угроз обнаружила серверы управления вредоносными программами (C2) в точках продаж (POS) для двух вариантов вредоносных программ, на которых размещено более 167 000 записей о платежах с украденных кредитных карт.

Кредитные карты были украдены в период с февраля 2021 г. по 8 сентября 2022 г. у эмитентов, в основном (97%), расположенных в Соединенных Штатах.

По словам исследователей Group-IB, на плохо сконфигурированном сервере размещалась административная панель для вредоносных программ MajikPOS и

Treasure Hunter. На панели MajiPOS было 77 428 дампов кредитных карт, а на панели охотников за сокровищами — 90 024.

IB-Group поделилась информацией с организацией по обмену финансовыми угрозами и правоохранительными органами внутри подразделения.

Украденные кредитные карты на сумму 3,3 миллиона долларов в даркнете

В период с апреля 2021 года по апрель 2022 года рынок украденных кредитных карт стоил около 908 713 251 долларов, при этом каждый сброс карты продавался по 20 долларов. Таким образом, злоумышленник заработает не менее 3,3 миллиона долларов на продаже украденных кредитных карт на подпольных хакерских форумах.

Однако базирующаяся в Сингапуре группа по анализу угроз не смогла определить, избавлялись ли хакеры от украденных кредитных карт на каком-либо форуме по киберпреступности.

Печально известные варианты вредоносного ПО для POS-терминалов существуют уже более пяти лет.

Вредоносное ПО MajikPOS впервые появилось в 2017 году и предназначалось для платежных устройств в США и Канаде, а Treasure Hunter впервые было обнаружено в 2014 году.

Веселый Роджер создал Treasure Hunter для российской хакерской группы BearsInc, которая управляла кардинговым форумом для продажи украденных кредитных карт. Однако позже исходный код зловреда просочился на русскоязычный хакерский форум в 2018 году и распространился среди других преступных группировок и исследователей безопасности. Вредоносное ПО Treasure Hunter POS нацелено на ОЗУ (оперативную память) зараженных устройств (скрапинг ОЗУ) для извлечения платежных данных и пересылки их на серверы C2.

Таким образом, шифрование данных в памяти может предотвратить атаки, хотя хакеры все же могут взломать некоторые алгоритмы шифрования.

«Конечно, следует учитывать традиционные методы шифрования, но некоторые алгоритмы можно легко взломать, а управление ключами и другие операционные проблемы делают простое шифрование данных непривлекательным», — сказал Эрфан Шадаби, эксперт по кибербезопасности в Comforte AG. «Имейте в виду, что зашифрованная информация не имеет исходного формата данных, поэтому корпоративные приложения должны быть либо изменены, либо данные должны быть защищены».

Шадаби рекомендовал использовать токенизацию для сохранения формата данных при сокрытии конфиденциальных элементов данных от парсеров оперативной памяти.

«Корпоративные приложения намного лучше поддерживают токенизированные данные, обходя необходимость снятия защиты информации для работы с ней в рамках корпоративного рабочего процесса».

Вредоносное ПО для POS-терминалов использует атаки грубой силы или украденные учетные данные для входа

Исследователи Group-IB объяснили, что операторы вредоносного ПО получают доступ, взламывая целевой POS-терминал или покупая учетные данные для входа у брокеров начального доступа.

Операторы MajikPOS обычно нацелены на плохо защищенные экземпляры VNC и RDP для доступа к платежным устройствам и установки вредоносных программ для POS.

Слишком рано списывать вредоносное ПО для POS-терминалов

Исследователи Group-IB Николай Шелехов и Саид Хамчиев отмечают, что вредоносное ПО для POS-терминалов стало менее привлекательным из-за мер безопасности, принятых карточной индустрией. Кроме того, злоумышленники применяют другие эффективные тактики, такие как анализаторы JavaScript, для сбора данных платежных карт с веб-сайтов электронной коммерции.

Однако они предупредили, что, хотя меньше преступников собирает данные с магнитных полос на платежных картах, дампы кредитных карт более ценны, чем текстовые данные кредитных карт.

«Учитывая, насколько они редки и для скольких различных мошеннических действий они могут быть использованы, дампы карт обычно обходятся дороже, чем текстовые данные карт», — заявили исследователи.

Исследователи IB-Group также пояснили, что мошенники не могут совершать прямые онлайн-покупки с использованием карточных дампов. Однако они могли клонировать украденные кредитные карты, снимать наличные в банкоматах или совершать покупки в обычных магазинах. Таким образом, эмитенты карт должны сохранять бдительность, чтобы обнаруживать украденные кредитные карты, прежде чем злоумышленники смогут модифицировать их для совершения покупок.

По словам исследователей, вредоносное ПО для POS представляло «серьезную угрозу» в регионах, где кредитные карты с магнитной полосой были основным механизмом обработки платежей, например в США.

«Учитывая, что вредоносное ПО остается активным на момент написания этого блога, число жертв продолжает расти», — предупреждают исследователи.

Майк Паркин, старший технический инженер Vulcan Cyber, отметил, что хотя безопасность POS-терминалов улучшилась, злоумышленники отказались отказаться от своей прежней тактики и «перешли к другим векторам для кражи информации о кредитных картах». ***(Alicia Hope. Over 167,000 Stolen Credit Cards Exposed on POS Malware Server // CPO Magazine (https://www.cpomagazine.com/cyber-security/over-167000-stolen-credit-cards-exposed-on-pos-malware-server/). 03.11.2022).***

***

«Геймеры и опытные пользователи Windows становятся мишенью поддельных порталов загрузки MSI Afterburner, чтобы заразить пользователей майнерами криптовалюты и вредоносной программой для кражи информации RedLine.

MSI Afterburner — это утилита для графического процессора, которая позволяет настраивать разгон, создавать профили вентиляторов, выполнять захват видео и отслеживать температуру установленных видеокарт и загрузку ЦП.

Утилита, созданная MSI, может использоваться пользователями практически всех видеокарт, что привело к ее использованию миллионами геймеров по всему миру, которые настраивают параметры для повышения производительности игр, делают свои графические процессоры более тихими и снижают температуру.

Однако популярность этого инструмента также сделала его хорошей мишенью для злоумышленников, которые хотят нацелиться на пользователей Windows с мощными графическими процессорами, которые можно использовать для майнинга криптовалюты.

Выдача себя за MSI Afterburner

Согласно новому отчету Cyble, за последние три месяца в сети появилось более 50 веб-сайтов, выдающих себя за официальный сайт MSI Afterburner.

В кампании использовались домены, которые могли заставить пользователей думать, что они посещают законный веб-сайт MSI, и которые легче продвигать с помощью BlackSEO. Некоторые из доменов, обнаруженных Cyble, перечислены ниже:

msi-afterburner--download.site
msi-afterburner-download.site
msi-afterburner-download.tech
msi-afterburner-download.онлайн
msi-afterburner-download.store
msi-afterburner-download.ru
msi-afterburner.download
msafterburners.com
msi-afterburnerr.com

В других случаях домены не напоминали бренд MSI и, вероятно, продвигались через прямые сообщения, форумы и сообщения в социальных сетях. Примеры включают:

git[.]git[.]skblxin[.]matrizauto[.]net
git[.]git[.]git[.]skblxin[.]matrizauto[.]net
git[.]git[.]git[.]git[.]skblxin[.]matrizauto[.]net
git[.]git[.]git[.]git[.]git[.]skblxin[.]matrizauto[.]net

Скрытый майнинг при краже ваших паролей

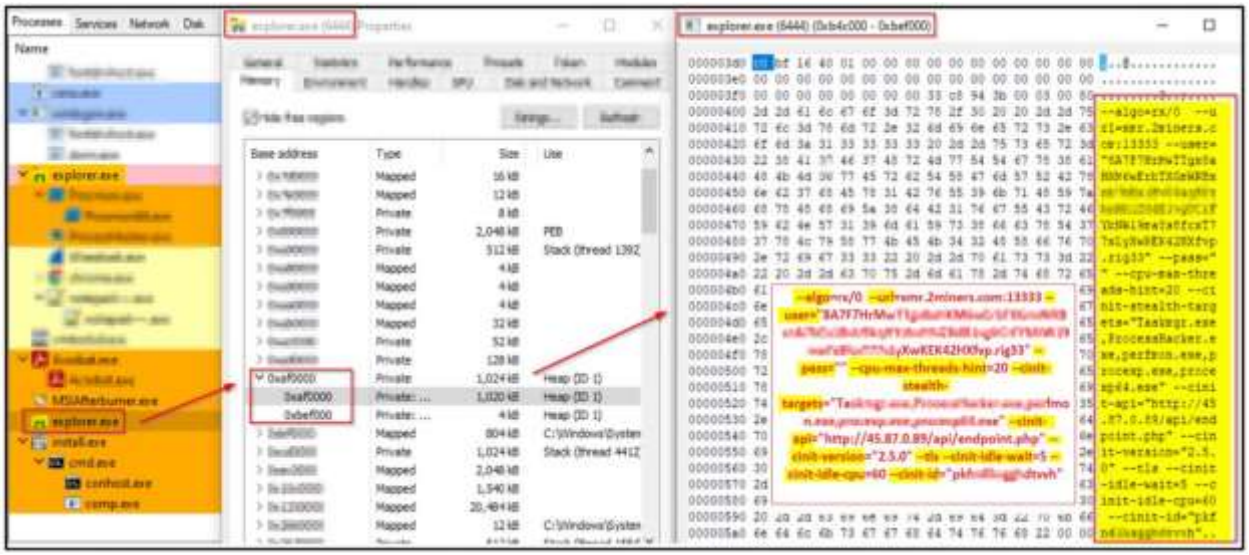
При запуске поддельного установочного файла MSI Afterburner (MSIAfterburnerSetup.msi) будет установлена подлинная программа Afterburner. Тем не менее, установщик также незаметно удалит и запустит вредоносное ПО RedLine для кражи информации и майнер XMR на скомпрометированном устройстве.

Майнер устанавливается через 64-битный исполняемый файл Python с именем «browser_assistant.exe» в локальном каталоге Program Files, который внедряет оболочку в процесс, созданный установщиком.

Этот шеллкод извлекает майнер XMR из репозитория GitHub и внедряет его непосредственно в память в процессе explorer.exe. Поскольку майнер никогда не прикасается к диску, шансы быть обнаруженным продуктами безопасности сведены к минимуму.

Майнер подключается к своему пулу майнинга, используя жестко заданное имя пользователя и пароль, а затем собирает и передает основные системные данные злоумышленникам.

Один из аргументов, который использует майнер XMR, — это «Максимальное количество потоков ЦП», установленное на 20, что превышает количество самых современных потоков ЦП, поэтому он настроен на захват всей доступной мощности.


Детали аргумента XMRminer (Cyble)

Майнер настроен на добычу только через 60 минут после перехода процессора в режим ожидания, что означает, что зараженный компьютер не выполняет никаких ресурсоемких задач и, скорее всего, остается без присмотра.

Кроме того, он использует аргумент «-cinit-stealth-targets», который позволяет приостановить активность майнинга и очистить память графического процессора при запуске определенных программ, перечисленных в разделе «невидимые цели».

Это могут быть мониторы процессов, антивирусные инструменты, средства просмотра аппаратных ресурсов и другие инструменты, которые помогают жертве обнаружить вредоносный процесс.

В этом случае приложения Windows, от которых пытается скрыться майнер, — это Taskmgr.exe, ProcessHacker.exe, perfmon.exe, procexp.exe и procexp64.exe.

В то время как майнер незаметно захватывает ресурсы вашего компьютера для майнинга Monero, RedLine уже работает в фоновом режиме, крадя ваши пароли, файлы cookie, информацию браузера и, возможно, любые криптовалютные кошельки.

К сожалению, почти все компоненты этой поддельной кампании MSI Afterburner плохо обнаруживают антивирусное программное обеспечение.

VirusTotal сообщает, что вредоносный установочный файл «MSIAfterburnerSetup.msi» обнаруживается только тремя продуктами безопасности из 56, а «browser_assistant.exe» обнаруживается только двумя продуктами из 67.

Чтобы обезопасить себя от майнеров и вредоносного ПО, загружайте инструменты непосредственно с официальных сайтов, а не с сайтов, опубликованных на форумах, в социальных сетях или в личных сообщениях.

В этом случае законный MSI Afterburner можно загрузить непосредственно с сайта MSI по адресу www.msi.com/Landing/afterburner/graphics-cards». ***(Bill Toulas. Fake MSI Afterburner targets Windows gamers with miners, info-stealers // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fake-msi-afterburner-targets-windows-gamers-with-miners-info-stealers/). 23.11.2022).***

***

«Более 1600 общедоступных образов Docker Hub скрывают вредоносное поведение, в том числе майнеры криптовалюты, встроенные секреты, которые можно использовать в качестве бэкдоров, угонщики DNS и перенаправители веб-сайтов.

Docker Hub — это облачная библиотека контейнеров, позволяющая людям свободно искать и загружать образы Docker или загружать свои творения в общедоступную библиотеку или личные репозитории.

Образы Docker — это шаблоны для быстрого и простого создания контейнеров, содержащих готовый к использованию код и приложения. Поэтому те, кто хочет настроить новые экземпляры, часто обращаются к Docker Hub, чтобы быстро найти легко развертываемое приложение.

К сожалению, из-за злоупотребления службой злоумышленниками более тысячи вредоносных загрузок представляют серьезную опасность для ничего не подозревающих пользователей, развертывающих загруженные вредоносным ПО образы в локально размещенных или облачных контейнерах.

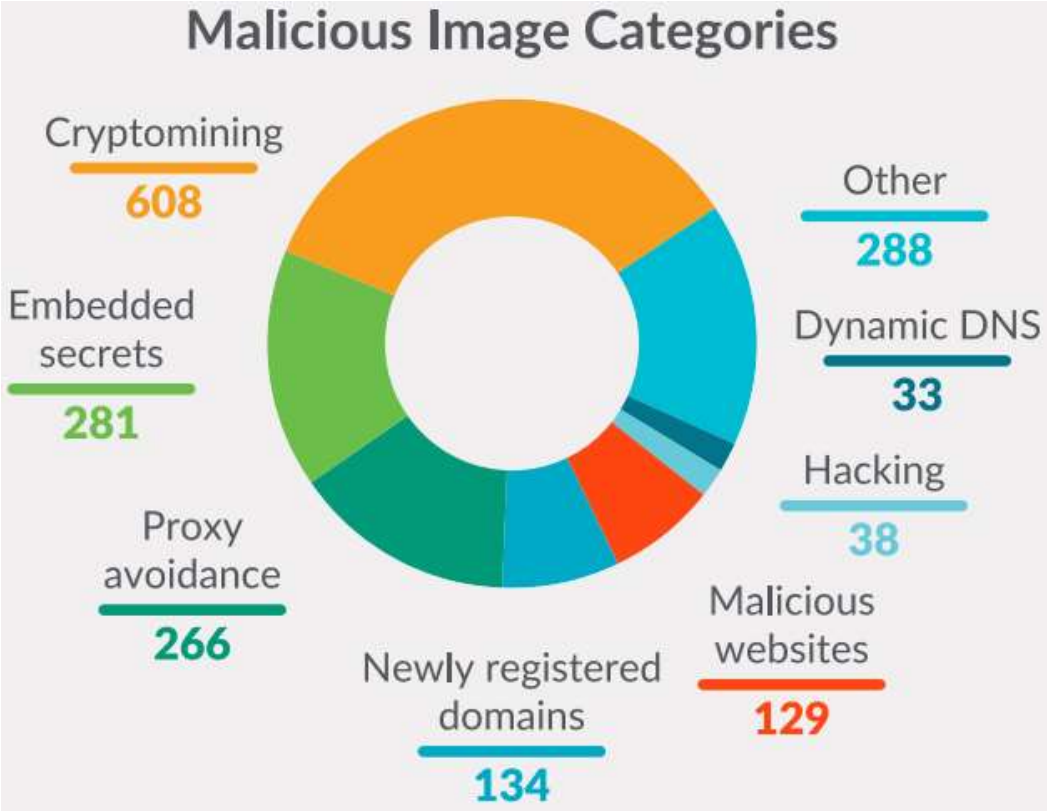
Многие вредоносные образы используют имена, которые маскируют их под популярные и заслуживающие доверия проекты, поэтому злоумышленники явно загрузили их, чтобы обманом заставить пользователей загрузить их.

Исследователи из Sysdig изучили проблему, пытаясь оценить масштаб проблемы, и сообщили о найденных изображениях, которые содержат вредоносный код или механизм в той или иной форме.

Ловушки Docker Hub

Помимо изображений, проверенных проектом Docker Library Project и проверенных на достоверность, на сервисе находятся сотни тысяч изображений с неизвестным статусом.

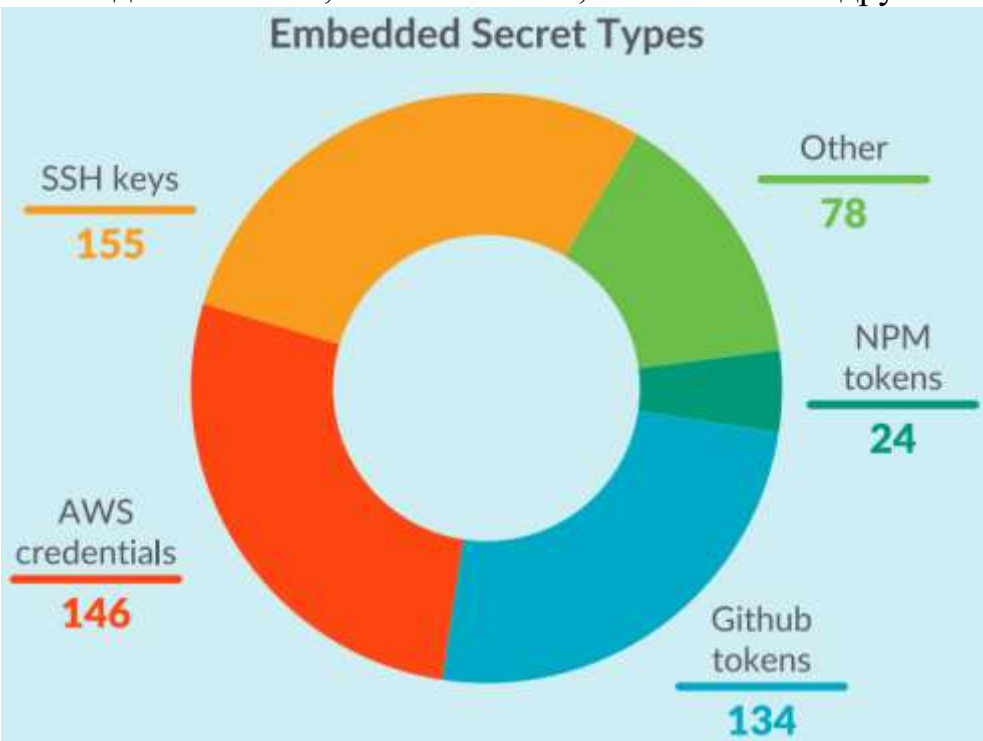
Sysdig использовала свои автоматизированные сканеры для тщательного изучения 250 000 непроверенных образов Linux и идентифицировала 1652 из них как вредоносные.



Типы вредоносных образов на Docker Hub (Sysdig)

Самой большой категорией были крипто-майнеры, обнаруженные в 608 образах контейнеров, которые использовали ресурсы сервера для майнинга криптовалюты для злоумышленников.

Вторым по частоте явлением были изображения, скрывающие встроенные секреты, насчитывающие 281 случай. Секреты, встроенные в эти образы, — это ключи SSH, учетные данные AWS, токены GitHub, токены NPM и другие.



Типы секретов, оставленных в образах Docker (Sysdig)

Sysdig отмечает, что эти секреты могли быть оставлены на общедоступных изображениях по ошибке или намеренно введены злоумышленником, который их создал и загрузил.

«Встраивая ключ SSH или ключ API в контейнер, злоумышленник может получить доступ после развертывания контейнера», — предупреждает Sysdig в отчете.

«Например, загрузка открытого ключа на удаленный сервер позволяет владельцам соответствующего закрытого ключа открывать оболочку и выполнять команды через SSH, аналогично внедрению бэкдора».

Многие вредоносные образы, обнаруженные Sysdig, использовали типосквоттинг, чтобы выдавать себя за законные и надежные изображения, только для заражения пользователей крипто-майнерами.

Эта тактика закладывает основу для некоторых очень успешных случаев, таких как два примера, показанные ниже, которые были загружены почти 17 000 раз.

Image Name	Image Digest	Downloads
vibersastra/ ubuntu	81b850230c2a9ea155aa06adda5537f5 e01a4ec2b0209aaa24c23e06161ff385	10,000+
vibersastra/ golang	a6af08adbcf9eba00e3ea15f8a67a7766 465fb387868efd43ab77f7668a8dc46	6,900

Образы Docker, содержащие майнеры монет (Sysdig)

Typosquatting также гарантирует, что пользователи, вводящие опечатку в названии популярного проекта, загрузят вредоносный образ, поэтому, хотя это не приводит к большому количеству жертв, оно по-прежнему обеспечивает постоянный поток заражений.

Image Name	Image Digest	Downloads
ynprpagamentitk/liferay	3978fb1b4d9581fddbd44f44901e87f9f8baf7942c74d5820c573c06cc83f861	281
arrghgluiistk/drupal	9ab7485664242c00db8ec6e0ea2b829320a7762107527a8c66d1754ec730c8b8	213
eiprtvchdcom/drupal	c7490c9e2a437e111968e96529cef80bc0d92a7040b656e2404114837e270941	131
vesnpsexga/joomla	3978fb1b4d9581fddbd44f44901e87f9f8baf7942c74d5820c573c06cc83f861	118
ganodndentcom/drupal	380898334e75e10cc1e5cf4c574d46e57f8b32f52552924fc1f5c158a7fb3291	55
dogigeronracom/drupal	50c1685bfcd67435188e74c8b5321de32f44f0c613fc2eebdbff3020273e690a	37
pumevnezdiroorg/drupal	bf9c24747d7c2903cf931a0a321f37c44fe6236dc40679d4cec3743384943e40	31

Опечатанные изображения, фиксирующие случайные опечатки (Sysdig)

Обострение проблемы

Sysdig сообщает, что в 2022 году 61% всех изображений, извлеченных из Docker Hub, поступят из общедоступных репозиториев, что на 15% больше, чем в 2021 году, поэтому риск для пользователей возрастает.

К сожалению, размер публичной библиотеки Docker Hub не позволяет ее операторам ежедневно проверять все загрузки; следовательно, о многих вредоносных изображениях не сообщается.

Sysdig также заметил, что большинство злоумышленников загружают только пару вредоносных изображений, поэтому даже если опасное изображение будет удалено, а загрузчик будет забанен, это не окажет существенного влияния на ландшафт угроз платформы». ***(Bill Toulas. Docker Hub repositories hide over 1,650 malicious containers // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/docker-hub-repositories-hide-over-1-650-malicious-containers/). 24.11.2022).***

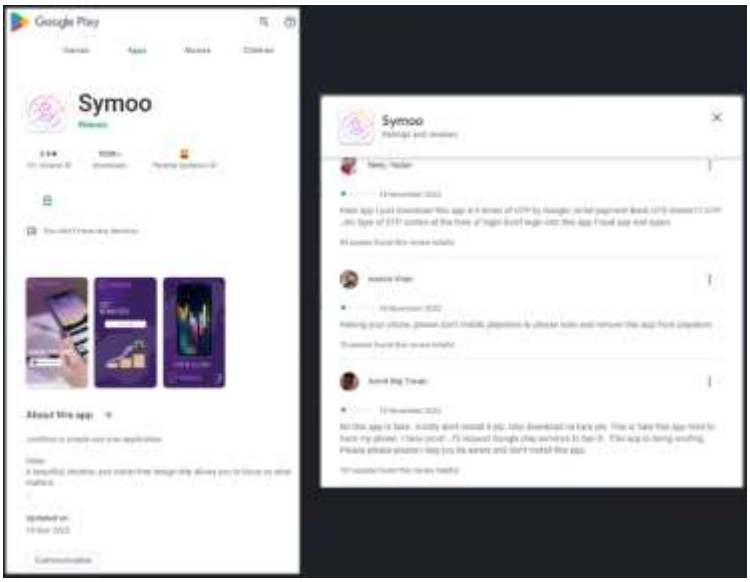
***

«Было обнаружено, что фальшивое SMS-приложение Android с 100 000 загрузок в магазине Google Play тайно действует как ретранслятор SMS для службы создания учетных записей для таких сайтов, как Microsoft, Google, Instagram, Telegram и Facebook.

Исследователь говорит, что зараженные устройства затем сдаются в аренду как «виртуальные номера» для передачи одноразового кода доступа, используемого для проверки пользователя при создании новых учетных записей.

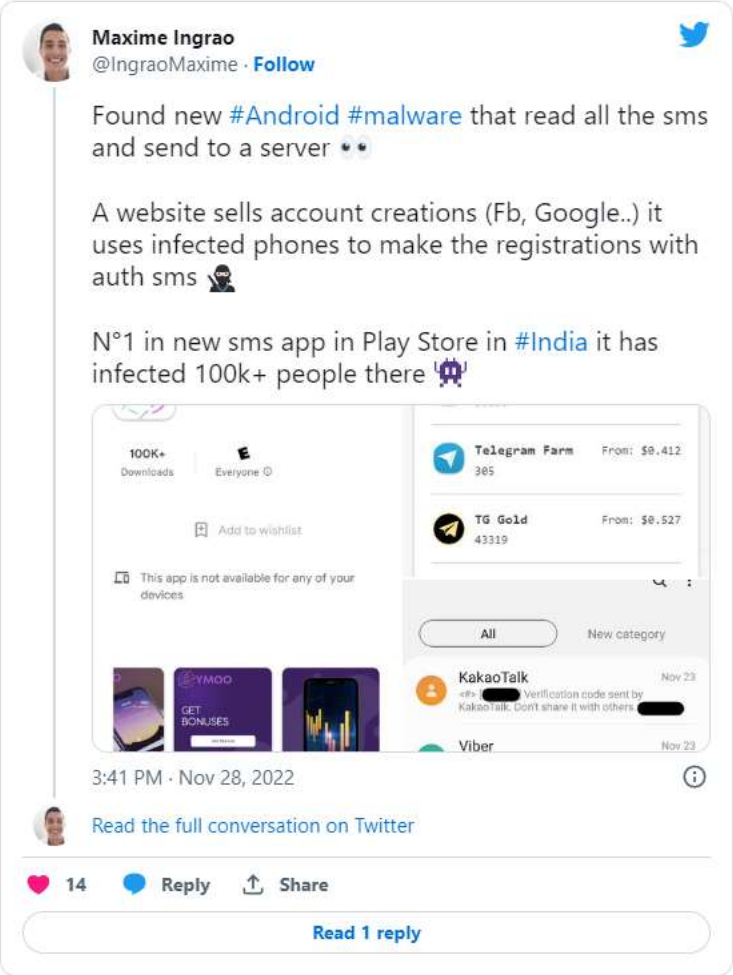
Хотя общий рейтинг приложения составляет 3,4, многие пользователи в отзывах жалуются, что оно является подделкой, взламывает их телефоны и генерирует несколько OTP (одноразовых паролей) при установке.

«Поддельное приложение. Я просто загружаю это приложение 4-5 раз OTP от Google, платеж Airtel, Bank OTP, dream11 OTP и т. д. Тип OTP приходит во время входа в систему», — говорится в одном из отзывов.



Приложение Symoo и отзывы пользователей в Google Play

Symoo был обнаружен исследователем безопасности Evina Максимом Инграо, который сообщил об этом в Google, но до сих пор не получил ответа от команды Android. На момент написания приложение остается доступным в Google Play.



BleepingComputer также связался с Google по поводу Symoo, и мы обновим эту историю, как только получим ответ.

Маршрутизация кодов 2FA

После установки на устройство приложение запрашивает доступ для отправки и чтения SMS, что звучит нормально, поскольку Symoo позиционирует себя как «простое в использовании» приложение для SMS.

На первом экране пользователю предлагается указать свой номер телефона; после этого он накладывает поддельный экран загрузки, который якобы показывает ход загрузки ресурсов.

Однако этот процесс затягивается, что позволяет удаленным операторам отправлять несколько SMS-сообщений 2FA (двухфакторная аутентификация) для создания учетных записей в различных службах, читать их содержимое и пересылать обратно операторам.

По завершении приложение зависнет, так и не достигнув обещанного интерфейса SMS, поэтому пользователи обычно удаляют его.

К этому времени приложение уже будет использовать номера телефонов пользователей Android для создания поддельных учетных записей на различных онлайн-платформах, и рецензенты говорят, что их сообщения теперь заполнены одноразовыми кодами доступа к учетным записям, которые они никогда не создавали.

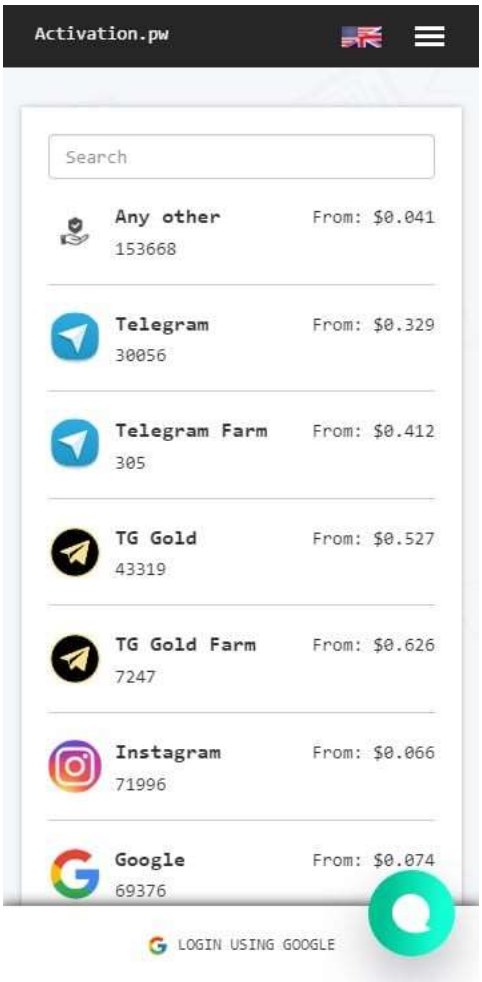
Продажа аккаунтов

Поскольку номера телефонов часто являются единственным возможным способом проверки учетных записей, люди, которые хотят участвовать в незаконных или анонимных действиях, находят эти псевдонимные учетные записи полезными.

Кроме того, Максим Инграо обнаружил, что приложение Symoo отправляет SMS-данные в домен, используемый другим приложением «Виртуальный номер», которое в какой-то момент также было в Google Play, но с тех пор было удалено.

Разработчик приложения «Виртуальный номер» также создал в Google Play еще одно приложение под названием «ActivationPW — Виртуальные номера», загруженное 10 000 раз, которое предлагает «Онлайн-номера из более чем 200 стран», которые вы можете использовать для создания учетной записи.

Используя это приложение, пользователи могут «арендовать» номер менее чем за 50 центов и во многих случаях использовать этот номер для проверки учетной записи.



АктивацияPW mobile GUI

Хотя это не подтверждено, считается, что приложение Symoo используется для получения и пересылки кодов подтверждения OTP, сгенерированных, когда люди создают учетные записи с помощью ActivationPW.

Если вы используете эти приложения, вам следует удалить их, по крайней мере, потому что они копируют содержимое ваших SMS на свои собственные серверы.

Их политика конфиденциальности также раскрывает это поведение, хотя они говорят, что это «блокировка спама и резервное копирование сервисов».

«Доходные SMS (мы храним смс как часть блока спама и резервируем сервисы с нашей сторонней платформой, облачным хранилищем или поставщиком услуг связи. (Обратите внимание, что мы не передаем эти записи третьим лицам)», — говорится в конфиденциальности Symoo политики». ***(Bill Toulas. Malicious Android app found powering account creation service // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/malicious-android-app-found-powering-account-creation-service/). 28.11.2022).***

***

«Хакеры извлекают выгоду из популярной задачи TikTok под названием «Invisible Challenge», чтобы установить вредоносное ПО на тысячи устройств и украсть их пароли, учетные записи Discord и, возможно, криптовалютные кошельки.

Новое и популярное задание TikTok требует, чтобы вы сняли себя обнаженным, используя фильтр TikTok «Невидимое тело», который удаляет тело из видео и заменяет его размытым фоном.

Эта проблема привела к тому, что люди публикуют видео, на которых они якобы обнажены, но скрыты фильтром.

Чтобы извлечь из этого выгоду, злоумышленники создают видеоролики TikTok, в которых утверждается, что они предлагают специальный «нефильтрующий» фильтр, удаляющий эффект маскировки тела TikTok и обнажающий обнаженные тела TikTokers.

Однако это программное обеспечение является поддельным и устанавливает вредоносное ПО «WASP Stealer (Discord Token Grabber)», способное украсть учетные записи Discord, пароли и кредитные карты, хранящиеся в браузерах, криптовалютные кошельки и даже файлы с компьютера жертвы.

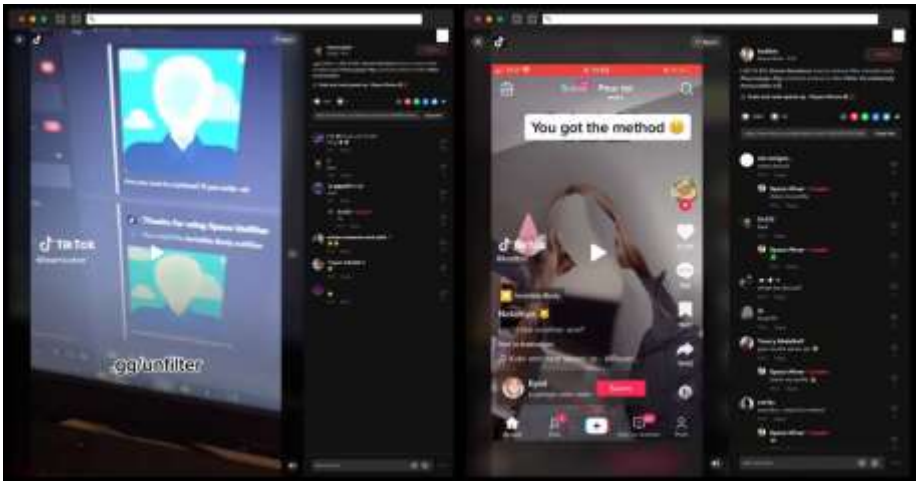
Эти видео набрали более миллиона просмотров вскоре после публикации, а один из серверов Discord злоумышленника собрал более 30 000 участников.

Ориентация на тренды TikTok

В новом отчете компании по кибербезопасности Checkmarx исследователи обнаружили два видеоролика TikTok, опубликованные злоумышленниками, которые быстро набрали более миллиона просмотров.

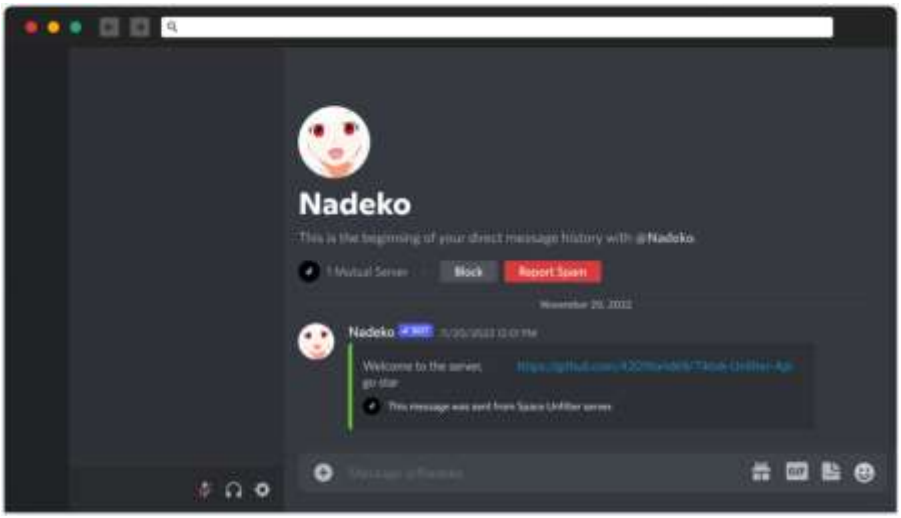
Пользователи TikTok @learncyber и @kodibtc создали видеоролики для продвижения программного приложения для «удаления невидимого тела фильтра», предлагаемого на сервере Discord под названием «Space Unfilter».

С тех пор злоумышленники переместили этот сервер Discord, но Checkmarx утверждает, что в какой-то момент у них было около 32 000 участников.



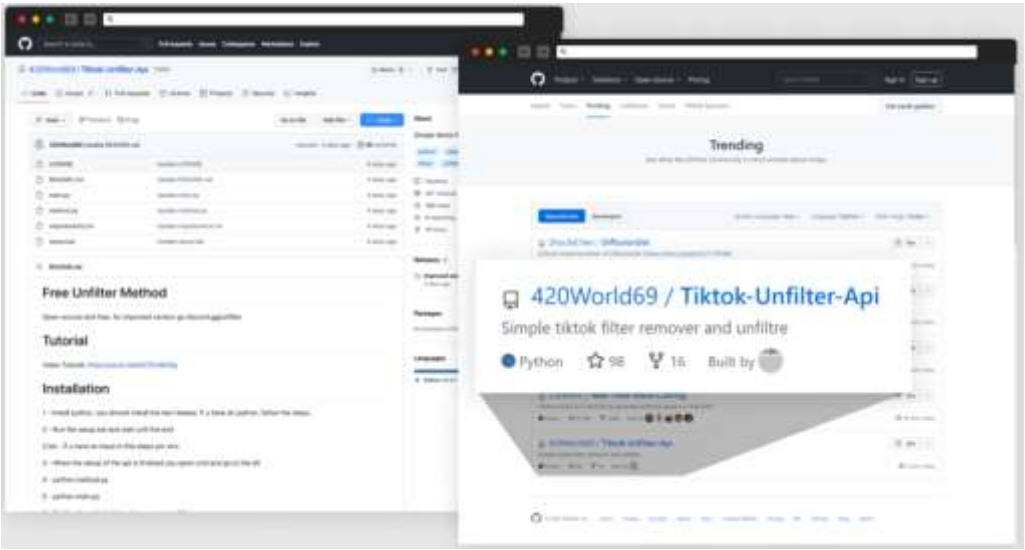
Видео TikTok, размещенные злоумышленниками (Checkmarx)

Как только жертвы подключаются к серверу Discord, они видят размещенную ботом ссылку, указывающую на репозиторий GitHub, в котором размещено вредоносное ПО.



Сервер Discord, использованный в атаках (Checkmarx)

Эта атака оказалась настолько успешной, что вредоносный репозиторий получил статус «популярного проекта GitHub», и хотя с тех пор он был переименован, в настоящее время он имеет 103 звезды и 18 форков.



Репозиторий GitHub с загрузчиком вредоносных программ (Checkmarx)

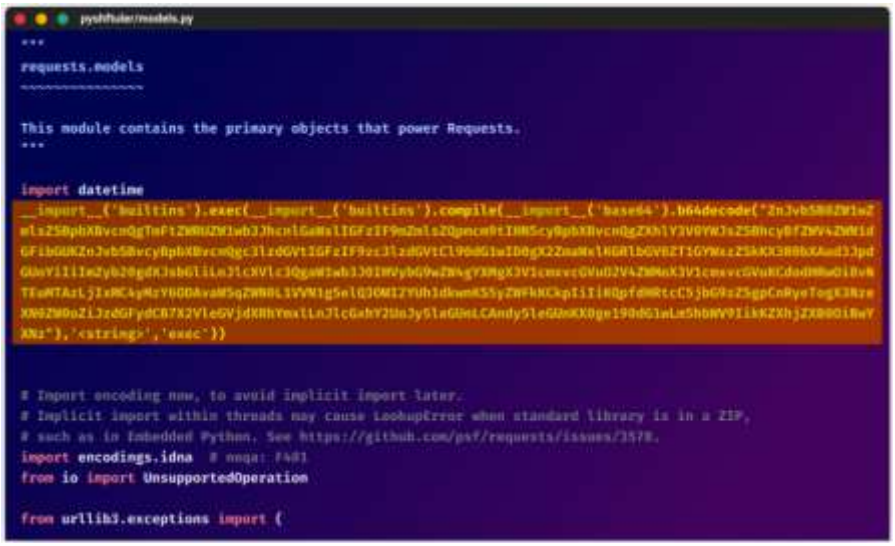
Файлы проекта содержали пакетный файл Windows (.bat), который при выполнении устанавливает вредоносный пакет Python (загрузчик WASP) и файл ReadMe, который ссылается на видео YouTube, содержащее инструкции по установке инструмента TikTok «unfilter».

Аналитики Checkmarx обнаружили, что злоумышленники использовали несколько пакетов Python, размещенных на PyPI, в том числе «tiktok-filter-api», «pyshftuler», «pyiopcs» и «pydesings», причем новые добавлялись каждый раз, когда сообщалось о старых пакетах и удалялись.

Кроме того, злоумышленники используют технику «StarJacking» в PyPI, связывая свой проект с популярным проектом GitHub, с которым они не связаны, чтобы сделать его законным.

Вредоносный пакет на PyPI (Checkmarx)

Вредоносный пакет копирует исходный код, но содержит модификацию для установки вредоносного ПО WASP на хост.



Вредоносная модификация кода (Checkmarx)

«Похоже, эта атака продолжается, и всякий раз, когда команда безопасности Python удаляет его пакеты, он быстро импровизирует и создает новую личность или просто использует другое имя», — говорится в отчете Checkmarx.

«Эти атаки еще раз демонстрируют, что кибер-злоумышленники начали сосредотачивать свое внимание на экосистеме пакетов с открытым исходным кодом; мы считаем, что эта тенденция только ускорится в 2023 году».

На момент написания этого репозиторий GitHub, используемый злоумышленником, все еще работал, но пакеты «TikTok unfilter» были заменены файлами «Nitro-генератора».

Сервер Discord «Unfilter Space» был отключен, а субъекты угрозы заявили, что перешли на другой сервер». ***(Bill Toulas. TikTok ‘Invisible Body’ challenge exploited to push malware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/tiktok-invisible-body-challenge-exploited-to-push-malware/). 28.11.2022).***

***

«Компания Group-IB обнаружила 34 киберпреступные группы, которые распространяют вредоносные программы — стилеры. По данным исследования, русскоговорящие злоумышленники использовали их для кражи паролей игровых аккаунтов в Steam и Roblox, «учеток» от торговой площадки Amazon и платежной системы PayPal, а также данных банковских карт и криптокошельков. Общей чертой групп является координация через телеграм-ботов на русском языке, однако атакуют они преимущественно иностранных пользователей из США, Бразилии и Индии. В 2022 году стилеры вновь становятся одной из самых серьезных угроз в сфере кибербезопасности.

Вышли из «Мамонта»

Отслеживая развитие популярной в России мошеннической схемы «Мамонт» (aka Classiscam), аналитики Group-IB Digital Risk Protection, обратили внимание на миграцию “воркеров” (так называют рядовых онлайн-жуликов) в более опасную преступную схему, связанную с распространением стилеров.

Стилеры — это вредоносное программное обеспечение (ВПО), которое «умеет» собирать с зараженного компьютера логины-пароли из учетных записей в браузерах, в том числе от почтовых сервисов или соцсетей, данные банковских карт, а также информацию о крипто-кошельках, а затем «передавать» все это своему оператору. После успешной атаки злоумышленники, как правило, идут двумя путями: либо сами «снимают» деньги, благодаря украденным данным, либо продают похищенную ими информацию на теневых формах. По оценкам специалистов Group-IB, в 2022 году стилеры являются одной из самых серьезных угроз в сфере кибербезопасности.

По данным Group-IB Threat Intelligence (входит в состав Unified Risk Platform), первые массовые группы и боты в Telegram, созданные для распространения стилеров, начали появляться в начале 2021 года. Проверка некоторых аккаунтов подтвердила версию, что участники нескольких мошеннических групп, специализирующихся ранее на схеме «Мамонт», стали работать со стилерам. В 2021-2022 годах эксперты Group-IB выявили в Telegram 34 действующие русскоязычные группы. Десять из них наиболее крупные — на каждую из них приходилось более 30 000 «отстуков», то есть сообщений от стилера, которые получает оператор с зараженной машины. В среднем в каждой группе состоит около 200 участников.

Переключившись с мошенничества на рассылку стилеров, злоумышленники не только копировали иерархию, модель, но и технические наработки «Мамонта». В первую очередь, речь идет о специальных телеграм-ботах, генерирующих вредоносный контент, коммуникацию между участниками и всю их теневую бухгалтерию. Задачи «воркеров» тоже изменились: теперь они должны нагнать трафик на сайт-приманку и заставить жертву скачать вредоносный файл.

Ссылку на скачивание стилеров злоумышленники чаще всего «зашивают» в видеообзоры популярных игр на YouTube, «софт» для майнига или NTF-файлы на специализированных форумах, розыгрыши и лотереи в соцсетях. По оценкам Group-IB, за 10 месяцев 2021 (с момента начала исследования 1 марта по 31 декабря) года пользователи более 538 000 раз скачали стилеры на свои компьютеры. В этом году ситуация ухудшилась. За первые 7 месяцев 2022 года (с 1 января до 1 августа) пользователи загрузили вирусные файлы более 890 000 раз.

Стилеры и где они обитают

Наиболее популярным стилером у изученных групп является RedLine — его использовали 23 из 34 команды. На втором месте Racoon — он стоит на вооружении в 8 командах. В 3 сообществах использовались самописные стилеры. Обычно администраторы предоставляли воркерам и Redline и Racoon бесплатно в обмен на долю похищенных данных или денежное вознаграждение, хотя на черном рынке аренда стилеров Redline и Racoon обходится в $150-200 в месяц. В отдельных группах используется сразу по 3 стилера, а в некоторых — только один.

По данным Group-IB, в 2021 году среди наиболее часто атакуемых сервисов фигурировали PayPal — более 25% и Amazon — более 18%. В 2022 году всё также лидируют PayPal (более 16%) и Amazon (более 13%). Однако за год почти в 5 раз увеличились случаи получения в логах паролей от игровых сервисов (Steam, EpicGames, Roblox).

Топ-3 наиболее атакуемых стран в 2022 году занимали США, Бразилия и Индия. Россия постепенно выбывает из списка приоритетов жуликов: если в 2021 года Россия занимала 15 место по числу пользователей, чьи пароли были украдены с помощью стилеров, то по итогам семи месяцев этого года РФ расположилась на 95-м месте.

За 10 месяцев 2021 года, по оценкам аналитиков Group-IB, злоумышленники из изученных групп получили 538 982 логов, 27 875 879 паролей, 1 215 532 572 куки-файла, данные от 56 779 карты, данные от 35 791 криптокошельков. За первые 7 месяцев 2022 года ими было украдено уже 896 148 логов, 50 352 518 паролей, 2 117 626 523 куки-файла, данные от 103 150 карты, данные от 113 204 криптокошельков. Реализовав на теневом рынке только логи и данные карт, злоумышленники, по оценкам экспертов Group-IB, могли заработать около 350 млн рублей или $5,8 млн.

«Приток огромного числа воркеров в популярную мошенническую схему «Мамонт» — на ее пике мы фиксировали более 1100 преступных групп и сотни тысяч фейковых сайтов — привел к конкуренции за ресурсы и поиску новых способов преступного заработка, — говорит Евгений Егоров, ведущий аналитик Group-IB Digital Risk Protection. — Популярности схемы с распространением стилеров способствует низкий порог входа: новичку не требуется технических знаний, поскольку процесс полностью автоматизирован через бота, а задача воркера сводится к тому, чтобы создать в телеграм-боте файл со стилером и «нагнать» на него трафик. Но для жертвы, чей компьютер заражен стилером, последствия могут быть очень серьезными».

Эксперты Group-IB Digital Risk Protection рекомендуют пользователям не загружать ПО из сомнительных источников, для установки лучше использовать изолированную виртуальную машину или альтернативную операционную систему, не сохранять пароли в браузере, регулярно чистить cookie данные браузеров для минимизации возможных рисков. Что касается компаний, то для избежания цифровых рисков и нежелательных последствий им стоит проактивно заниматься цифровой безопасностью своего бренда и использовать современные технологии для мониторинга и реагирования». ***(Русскоязычные операторы атакуют иностранных пользователей Steam, Roblox, Amazon и PayPal // ИКС-МЕДИА (https://www.iksmedia.ru/news/5922750-Russkoyazychnye-operatory-atakuyut.html). 23.11.2022).***

***

«Вредоносное ПО — это общий термин, который включает все типы вредоносного программного обеспечения, включая вирусы, черви, трояны, программы-вымогатели и программы-шпионы. Эти программы предназначены для заражения и повреждения компьютеров, кражи конфиденциальных данных или получения контроля над системой. В 2022 году 75% организаций столкнулись с

активностью вредоносного ПО, которое распространялось между сотрудниками, что является самым высоким показателем за последние годы. Как только вредоносное ПО получает доступ к системе, под угрозой оказывается не только пострадавшее устройство, но и все остальные устройства в той же сети. Для простоты мы будем использовать преимущественно компьютеры в качестве примеров, однако важно осознавать тот факт, что вредоносное ПО может поражать все типы цифровых устройств, включая настольные компьютеры, мобильные устройства и другие устройства Интернета вещей (IoT). Данные SonicWall Capture Labs показали, что в первой половине 2022 года количество атак вредоносных программ увеличилось на 11% по сравнению с 2021 годом, что составило около 2,8 миллиарда атак по всему миру. Кроме того, в течение 2022 года 35% респондентов заявили, что в случае кибератак, нарушающих работу их бизнеса, виновата плохая готовность. Поэтому важно принять необходимые меры предосторожности для защиты вашего устройства, установив соответствующую защиту от вредоносных программ и распознав признаки зараженной системы.

Как вредоносное ПО заражает компьютер?

Вредоносное ПО может заразить компьютер несколькими способами, в том числе через вложения электронной почты, веб-сайты и загрузку зараженного программного обеспечения. Вот некоторые из наиболее распространенных способов заражения вашего компьютера вредоносными программами.

Вредоносные или скомпрометированные веб-страницы

Вредоносная веб-страница — это веб-страница, предназначенная для заражения вашего компьютера вредоносными программами. Вредоносные веб-страницы создаются киберпреступниками или могут быть результатом компрометации законного веб-сайта (также известного как взлом). Вредоносные веб-страницы могут заразить ваш компьютер вредоносными программами, если вы посещаете их, переходите по ссылкам или загружаете с них файлы. Обычный способ, с помощью которого киберпреступники заставляют своих жертв посещать вредоносные веб-страницы, заключается в рассылке большого количества мошеннических электронных писем, обычно называемых фишинговыми электронными письмами.

Распознавание вредоносных веб-страниц

Лучший способ не стать жертвой заражения — знать, как распознать вредоносную веб-страницу. Есть несколько явных признаков того, что веб-страница может быть вредоносной.

Во-первых, обратите внимание на URL-адрес: фальшивая ссылка может выглядеть странно и совсем не похоже на легитимный домен, за который она якобы выдает себя. Другие, более сложные примеры могут содержать орфографические ошибки известных веб-сайтов, поэтому всегда следите за ними. Ссылки перенаправления, пожалуй, самые эффективные из вредоносных ссылок, так как это ссылки, которые выглядят нормально, но перенаправляют на другой сайт. Вы можете определить ссылку перенаправления, проверив ее фактическое назначение с помощью онлайн-инструментов.

Во-вторых, оказавшись на странице, может стать очевидным, что что-то не так, поскольку вы можете обнаружить, что на ней мало контента или он отсутствует.

Другими признаками поддельной веб-страницы являются грамматические и орфографические ошибки. Однако будьте осторожны, так как некоторые вредоносные веб-сайты могут выглядеть почти так же, как их законные аналоги.

В-третьих, веб-страница может рекламировать продукты или услуги, которые кажутся слишком хорошими, чтобы быть правдой. Всплывающие окна, появляющиеся часто, иногда настолько часто, что использование страницы превращается в кошмар, также являются признаками того, что страница может быть гнусной.

Если вы столкнулись с любым из этих признаков, лучше немедленно покинуть страницу. Для дополнительной безопасности вы также можете очистить кеш браузера и файлы cookie.

Фишинговые и целевые фишинговые письма

Распространенной стратегией, которую киберпреступники используют для заражения компьютерной системы жертвы, является рассылка фишинговых писем. Фишинговая электронная почта — это кибератака с использованием социальной инженерии, целью которой является обманным путем заставить жертв предоставить конфиденциальную информацию, такую как учетные данные для входа или номера кредитных карт. Киберпреступники часто выдают себя за законную компанию или частное лицо, чтобы завоевать доверие жертвы. Примером фишингового электронного письма может быть электронное письмо от технической компании, в котором говорится о проблеме с вашей учетной записью и предлагается щелкнуть ссылку, по которой вы можете установить последнее обновление для системы безопасности. Однако это оказывается вредоносной ссылкой, ведущей на зараженный вредоносным ПО веб-сайт. Фишинговое электронное письмо может также попросить получателя заполнить прикрепленную регистрационную форму.

Целевой фишинг — это более целенаправленная версия фишинга, при которой киберпреступники проводят свои исследования и нацелены на конкретного человека или организацию. Они часто используют личную информацию о жертве, такую как ее имя, должность или интересы, чтобы сделать электронное письмо более достоверным. Примером целевого фишинга может быть электронное письмо, якобы отправленное вашим начальником, с просьбой обновить ваши личные данные на зараженном вредоносным ПО веб-сайте или в программном обеспечении.

Распознавание фишинговых писем

Фишинговые электронные письма может быть трудно обнаружить, поскольку они часто выглядят законными. Тем не менее, есть некоторые явные признаки того, что электронное письмо является попыткой фишинга. Во-первых, проверьте адрес электронной почты отправителя. Фишинговое электронное письмо часто имеет поддельный или поддельный адрес, похожий на настоящий адрес. Во-вторых, ищите опечатки или грамматические ошибки в теле письма. Это может указывать на то, что электронное письмо отправлено не из законного источника. В-третьих, будьте осторожны с любыми электронными письмами, которые создают ощущение срочности или требуют от вас немедленных действий, например, нажатия на ссылку. Наконец, если в электронном письме запрашивается личная информация, такая как ваши учетные данные для входа или номер кредитной карты, это верный признак того, что это фишинговое письмо.

Классическая фишинговая электронная почта — это письмо нигерийского принца, которому нужна помощь в переводе своего состояния из страны. В этих письмах часто запрашивают данные вашего банковского счета, чтобы деньги могли быть переведены вам. Однако это не что иное, как мошенничество.

Адресные фишинговые электронные письма часто гораздо сложнее распознать, поскольку они могут быть очень персонализированными. Тем не менее, если вы получаете электронное письмо от любимого человека с просьбой о деньгах, всегда будьте подозрительны. Если вы не уверены в электронном письме, всегда лучше проявить осторожность и не нажимать на какие-либо ссылки или открывать какие-либо вложения. Если электронное письмо отправлено из законного источника, например, от вашего начальника или компании, с которой вы ведете бизнес, вы всегда можете связаться с ними напрямую, чтобы подтвердить, что электронное письмо является законным…

Зараженные съемные диски

Другой, менее распространенный способ заражения системы вредоносным ПО — это подключение зараженного внешнего диска к своему устройству незнакомым человеком. Иногда злоумышленники оставляют зараженный USB-накопитель в общественном месте, надеясь, что кто-нибудь из любопытства возьмет его и подключит к компьютеру. Вредоносное ПО будет автоматически установлено при подключении зараженного диска к вашей системе. Всегда с подозрением относитесь к съемным дискам, которые не принадлежат вам.

Как я могу обнаружить атаку вредоносного ПО и отреагировать на нее?

Предотвращение вредоносного ПО

Первым шагом к защите от любого типа вредоносного ПО всегда является профилактика. Злоумышленники могут нанести ущерб только в том случае, если им разрешено выполняться в системе, поэтому лучший способ остановить вредоносное ПО — вообще никогда не позволять ему запускаться. Один из самых простых способов сделать вашу систему менее уязвимой — просто обновлять операционную систему и программное обеспечение с помощью последних исправлений безопасности. Кроме того, установите надежную внешнюю антивирусную программу и сканер и следите за тем, чтобы они обновлялись с помощью последних определений вредоносных программ.

Обнаружение вредоносных программ

Как правило, наиболее эффективным способом обнаружения вредоносных программ являются инструменты, которые могут сканировать вашу систему на наличие известных сигнатур вредоносного кода. Эти методы обнаружения на основе сигнатур не являются надежными, поскольку вредоносное ПО может мутировать и изменять свой код, чтобы избежать обнаружения. В конечном счете, одним из последних уровней защиты является пользователь и его собственная способность определять необычное поведение. Конечно, разные типы вредоносного ПО часто имеют свои уникальные признаки. Ниже мы подробно остановимся на контрольных признаках двух основных типов вредоносных программ: программ-вымогателей и программ-шпионов.

Удаление вредоносных программ

Если вы считаете, что ваш компьютер уже заражен вредоносным ПО, первое, что вы должны сделать, это отключить зараженное устройство от Интернета, чтобы предотвратить дальнейший ущерб. Затем запустите полную проверку вашей системы с помощью антивирусной программы и удалите все обнаруженные вредоносные программы. Если вы не знаете, как это сделать, вы обычно можете найти инструкции, выполнив поиск вашей конкретной антивирусной программы в Интернете. Наконец, измените все пароли, которые могли быть скомпрометированы, и подумайте о том, чтобы обратиться за помощью к специалисту.

Шпионское ПО тайно следит за вашей активностью.

Что такое шпионское ПО?

Шпионское ПО — это тип вредоносного ПО, которое отслеживает действия вашего компьютера. Как только шпионское ПО заражает операционную систему, оно начинает отслеживать действия, связанные с этим устройством, регистрируя важную информацию, такую как пароли и другую интернет-активность, включая посещенные сайты, учетные записи в социальных сетях и даже финансовую информацию. Некоторые шпионские программы могут даже взять под контроль определенные функции зараженной системы, такие как веб-камера или микрофон, для записи аудио- и видеоматериалов без ведома жертвы. Затем эта информация передается киберпреступнику, который стоит за гнусной программой. С 2017 года количество обнаружений вредоносных программ предприятиями увеличилось на 79%, причем многие из них связаны с программами для кражи информации, такими как шпионское ПО.

Как я могу обнаружить атаку шпионского ПО и отреагировать на нее?

Предотвращение шпионского ПО

Есть несколько вещей, которые вы можете сделать, чтобы предотвратить заражение вашей системы шпионскими программами. Во-первых, как мы упоминали ранее, важно постоянно обновлять операционную систему и программное обеспечение с помощью последних исправлений безопасности. Это поможет закрыть любые потенциальные уязвимости, которые могут быть использованы вредоносными программами. Кроме того, установите надежную внешнюю антивирусную программу и сканер и следите за тем, чтобы они обновлялись с помощью последних определений вредоносных программ.

Обнаружение шпионского ПО

Общеизвестно, что шпионское ПО трудно обнаружить, поскольку оно спроектировано таким образом, чтобы избежать обнаружения традиционными мерами безопасности. Лучший способ защитить себя от программ-шпионов — знать о признаках того, что ваша система может быть заражена. Это могут быть необычные действия в вашей системе, такие как появление новых программ, которые вы не устанавливали, изменения домашней страницы или других важных настроек. Если вы заметили какой-либо из этих красных флажков, важно как можно скорее запустить сканирование вашей системы на наличие вредоносных программ.

Удаление шпионского ПО

Если вы считаете, что ваше устройство уже заражено шпионским ПО, самый быстрый способ предотвратить отправку дополнительной информации

злоумышленникам — отключить интернет. Это предотвратит связь вредоносной программы со своим сервером управления и контроля (C2). Затем запустите полную проверку вашей системы с помощью антивирусной программы и удалите все обнаруженные вредоносные программы. Если вы не знаете, как это сделать, вы обычно можете найти инструкции, выполнив поиск вашей конкретной антивирусной программы в Интернете. Наконец, измените все пароли, которые могли быть скомпрометированы, и подумайте о том, чтобы обратиться к профессионалу.

Примеры шпионского ПО

Примером шпионского ПО может служить программа, используемая в условиях корпоративного шпионажа, когда компьютер сотрудника заражается вредоносным ПО, которое отслеживает его действия и отправляет эту информацию обратно киберпреступнику. Затем эта информация может быть использована для доступа к конфиденциальной информации о корпорации, включая коммерческую тайну или данные учетной записи. Известным примером шпионского ПО является Pegasus, разработанное компанией NSO Group, производящей кибероружие. Программа используется как авторитарными, так и демократическими правительствами для слежки за высокопоставленными лицами, такими как журналисты, правозащитники и политические оппоненты, путем заражения их iPhone. Это вызвало критику группы NSO со стороны ООН за то, что она представляет угрозу свободе мнений.

Программа-вымогатель блокирует ваш доступ и угрожает уничтожить ваш носитель.

Что такое программы-вымогатели?

Программа-вымогатель — это тип вредоносного ПО, которое подвергает риску личные данные, угрожая уничтожить их, если требование о выкупе не будет выполнено. Атака программы-вымогателя зашифрует файлы на вашем компьютере, сделав их недоступными для вас. Киберпреступник, развертывающий программу-вымогатель, затем отправляет записку с требованием выкупа, обычно прося жертву заплатить выкуп в криптовалюте, чтобы расшифровать данные и восстановить доступ к файлам пользователя. В некоторых случаях киберпреступник может угрожать полностью уничтожить данные пользователя, если выкуп не будет уплачен. Часто программы-вымогатели не разрабатываются и не поддерживаются самим злоумышленником, а покупаются у третьей стороны. Это называется Ransomware-as-a-Service (Raas). В этой настройке программа-вымогатель разрабатывается и поддерживается разработчиком вредоносного ПО, который затем продает ее преступникам, которые продолжают использовать ее для вымогательства у своих жертв. В 2021 году 61 % организаций пострадали от кибератак, связанных с программами-вымогателями, которые привели как минимум к частичному нарушению работы. В конечном счете, программы-вымогатели закончили 2021 год, набрав 20 миллиардов долларов по всему миру, что обошлось предприятиям в среднем в 1,85 миллиона долларов. Кроме того, только 57% предприятий могут восстановить свои данные с помощью резервной копии.

Как я могу обнаружить атаку программы-вымогателя и отреагировать на нее?

Защита от программ-вымогателей

Как и в случае с любым другим вредоносным ПО, лучший способ блокировать атаки программ-вымогателей — постоянно обновлять систему с помощью последних исправлений безопасности и устанавливать проверенную антивирусную программу.

Другой, часто упускаемый из виду метод минимизации ущерба — регулярное резервное копирование данных, которые хранятся без подключения к вашему компьютеру, либо на внешнем жестком диске, либо в облачном хранилище. При этом последствия активного заражения вымогателями могут быть уменьшены, так как при этом вся информация на пораженном компьютере будет потеряна, а данных резервной копии не будет.

Обнаружение программ-вымогателей

Как и большинство вредоносных программ, бездействующие программы-вымогатели выдают себя, замедляя работу компьютера, создавая всплывающие окна и приложения, которые вы не устанавливали, и даже вызывая сбой компьютера. Однако к тому времени, когда программы-вымогатели обнаруживаются, часто бывает уже слишком поздно. Пользователю обычно предоставляется экран с требованием выкупа, чтобы восстановить доступ к вашему компьютеру.

Удаление программ-вымогателей

К сожалению, нет гарантированного способа удалить программы-вымогатели и расшифровать файлы, даже заплатив требуемый выкуп. Тем не менее, некоторые исследователи вредоносных программ смогли разработать бесплатные инструменты для удаления программ-вымогателей, которые могут работать в определенных случаях. Если вы считаете, что ваше устройство уже заражено программой-вымогателем, лучше всего немедленно отключиться от Интернета и сети, чтобы предотвратить распространение вредоносного ПО и дальнейшее шифрование файлов. Затем попробуйте запустить сканирование с помощью бесплатного инструмента для удаления программ-вымогателей. Если это не сработает, вам, вероятно, придется заплатить выкуп, чтобы вернуть свои данные. В случае компаний юристы захотят, чтобы с ними связались по поводу политики киберстрахования компании (если применимо) до выплаты выкупа. Кроме того, важно отметить, что некоторые субъекты угроз в Соединенных Штатах находятся под санкциями — обязательно проверьте их перед отправкой платежа. Наконец, измените все пароли, которые могли быть скомпрометированы, и обратитесь к специалисту, если вы не знаете, как действовать дальше…

Программы-вымогатели и программы-шпионы: основные выводы

Вредоносное ПО — это широкий термин, охватывающий различные типы вредоносного программного обеспечения, в том числе программы-вымогатели и программы-шпионы. Программа-вымогатель — это тип вредоносного ПО, которое подвергает риску личные данные, угрожая зашифровать или уничтожить их, если требование о выкупе не будет выполнено. Программа-вымогатель быстро даст о себе знать. Шпионское ПО, с другой стороны, представляет собой тип вредоносного ПО, которое отслеживает вашу активность и отправляет эту информацию обратно киберпреступнику, который затем может использовать конфиденциальную информацию для кражи денег у жертвы и/или совершения кражи личных данных. Лучший способ блокировать атаки вредоносных программ — постоянно обновлять

систему с помощью последних исправлений безопасности и устанавливать проверенную антивирусную программу. Если вы считаете, что ваше устройство уже заражено вредоносным ПО, лучше всего немедленно отключиться от Интернета, чтобы вредоносная программа не связалась со своим C2-сервером и не навредила вашему устройству и информации. Наконец, обязательно измените все пароли, которые могли быть скомпрометированы, и обратитесь к специалисту, если вы не знаете, как действовать дальше». ***(Malware, Spyware, and Ransomware: How They Differ and How to Respond // Ankura Consulting Group, LLC. (https://angle.ankura.com/post/102i0wt/malware-spyware-and-ransomware-how-they-differ-and-how-to-respond). 08.11.2022).***

***

Програми-вимагачі

«ЕС принял участие в Саммите инициативы по борьбе с программами-вымогателями 2022 года в Вашингтоне, округ Колумбия, 31 октября и 1 ноября, чтобы укрепить международное сотрудничество по борьбе с программами-вымогателями.

На втором саммите Инициативы по борьбе с программами-вымогателями, или CRI, участники — Австралия, Австрия, Бельгия, Бразилия, Болгария, Канада, Хорватия, Чехия, Доминиканская Республика, Эстония, Франция, Германия, Индия, Ирландия, Израиль, Италия, Япония., Кения, Литва, Мексика, Нидерланды, Новая Зеландия, Нигерия, Норвегия, Польша, Республика Корея, Румыния, Сингапур, Южная Африка, Испания, Швеция, Швейцария, Объединенные Арабские Эмираты, Великобритания, США, Украина и, недавно присоединившаяся Бельгия – подтвердила свои совместные обязательства по противодействию всем элементам угроз программ-вымогателей и обсудила следующие шаги. Они обязуются продолжать наращивать коллективную устойчивость к программам-вымогателям, сотрудничать в борьбе с программами-вымогателями и преследовать ответственных лиц, противодействуя незаконному финансированию, лежащему в основе экосистемы программ-вымогателей.

Для достижения вышеуказанных целей члены обязуются постоянно действовать, а именно:

Привлекать злоумышленников к ответственности за их преступления и не предоставлять им безопасное убежище

Бороться со способностью субъектов программ-вымогателей получать прибыль от незаконных доходов путем внедрения и обеспечения соблюдения мер по борьбе с отмыванием денег и противодействию финансированию терроризма (AML/CFT), включая правила «знай своего клиента» (KYC) для виртуальных активов и поставщиков услуг виртуальных активов.

Пресекать и привлекать к ответственности лиц, занимающихся программами-вымогателями, и их пособников в максимально возможной степени, разрешенной действующим законодательством каждого партнера и соответствующими органами.

Сотрудничать в борьбе с программами-вымогателями путем обмена информацией, где это уместно и в соответствии с применимыми законами и правилами, о неправомерном использовании инфраструктуры для запуска атак программ-вымогателей, чтобы гарантировать, что национальная киберинфраструктура не используется в атаках программ-вымогателей.

Более того, члены подвели итоги работы пяти рабочих групп, созданных в рамках этой инициативы, а именно рабочих групп по устойчивости, дипломатии, подрывным действиям, противодействию незаконному финансированию и государственно-частному партнерству.

Программы-вымогатели являются приоритетной задачей ЕС, и ЕС стремится бороться с программами-вымогателями в различных областях (устойчивость, дипломатия, сбои, незаконное финансирование). Для повышения устойчивости и борьбы с атаками программ-вымогателей требуется трансграничное сотрудничество для разработки инструментов, обмена информацией, повышения осведомленности и предотвращения кибератак». ***(International Counter Ransomware Initiative: strengthening cybersecurity cooperation & actions // Shaping Europe's digital future (https://digital-strategy.ec.europa.eu/en/news/international-counter-ransomware-initiative-strengthening-cybersecurity-cooperation-actions). 03.11.2022).***

***

«Три дюжины стран, но не Россия, обещают сотрудничество и принимают жесткие меры

Соединенные Штаты, Европейский Союз и три десятка стран пообещали принять жесткие меры против программ-вымогателей после двухдневной встречи в Белом доме.

Встреча была посвящена годовщине Международной инициативы по борьбе с программами-вымогателями, возглавляемой администрацией Байдена. Американские официальные лица утверждают, что за последние 12 месяцев удалось добиться прогресса, даже несмотря на то, что программы-вымогатели продолжают сеять хаос, влияя на уход за пациентами в одном из медицинских учреждений. Крупнейшие сети больниц Америки или требования о вымогательстве, выдвинутые против крупнейшей частной страховой компании Австралии. Во вторник министерство финансов подсчитало, что фактические выплаты или попытки выплат программ-вымогателей финансовыми учреждениями США в 2021 году составили почти 1,2 миллиарда долларов.

«Мы были свидетелями уничтожения», — сказал высокопоставленный чиновник администрации в ходе пресс-конференции в воскресенье вечером, указывая на арест и недавний приговор канадскому члену банды, занимающейся программами-вымогателями как услугой. Тем не менее, «мы видим, что темпы и изощренность атак программ-вымогателей растут быстрее, чем наши усилия по обеспечению устойчивости и разрушению», — признал чиновник.

В совместной декларации во вторник участники инициативы заявили, что они гарантируют, что хакерам-вымогателям не будет предоставлено безопасное убежище. Они обязались нацелиться на способность хакеров получать прибыль от

вымогательства, применяя требования «знай своего клиента» для торговых платформ криптовалюты.

В декларации говорится, что добровольная Международная целевая группа по борьбе с программами-вымогателями, возглавляемая Австралией, будет обмениваться ранними предупреждающими признаками атак программ-вымогателей, «а также консолидировать политику и рамки передового опыта».

Региональный центр киберзащиты в Литве проверит концепцию целевой группы, внедрив упрощенную версию оперативного обмена информацией об угрозах программ-вымогателей.

В число 36 стран, участвующих в инициативе, входит Украина — страна со своей долей доморощенных финансово мотивированных хакеров — но не входит Россия, эпицентр операций с программами-вымогателями.

Во время первого заседания инициативы в 2021 году высокопоставленный чиновник администрации заявил, что Россия не была приглашена, но оставил дверь открытой для возможного приглашения в будущем. Тот же чиновник в воскресенье отверг эту возможность, заявив, что эта инициатива «не столько связана с Россией, сколько с тем, как мы, как группа стран, усложняем, удорожаем и делаем более рискованными действия субъектов программ-вымогателей».

В совещании по вымогателям также приняли участие 13 компаний и организаций частного сектора, в том числе опоры безопасности Microsoft, Crowdstrike, Mandiant и Palo Alto Networks, некоммерческие организации Cyber Threat Alliance, Cybersecurity Coalition и Институт безопасности и технологий. Также присутствовали Flexxon, SAP, Siemens, Internet 2.0, Tata Consultancy Services и Telefónica». ***(David Perera. White House Ransomware Confab Ends With Data Sharing Pledge // Information Security Media Group, Corp. (https://www.govinfosecurity.com/white-house-ransomware-confab-ends-data-sharing-pledge-a-20386). 01.11.2022).***

***

«На втором саммите CRI участники подтвердили совместную приверженность созданию коллективной устойчивости к программам-вымогателям.

Члены Международной инициативы по борьбе с программами-вымогателями (CRI) — Австралия, Австрия, Бельгия, Бразилия, Болгария, Канада, Хорватия, Чехия, Доминиканская Республика, Эстония, Франция, Германия, Индия, Ирландия, Израиль, Италия, Япония, Кения, Литва, Мексика, Нидерланды, Новая Зеландия, Нигерия, Норвегия, Польша, Республика Корея, Румыния, Сингапур, Южная Африка, Испания, Швеция, Швейцария, Объединенные Арабские Эмираты, Великобритания, США и Украина, а также Европейский Союз — встретились в Вашингтоне, округ Колумбия, 31 октября — 1 ноября 2022 г. Ранее участвующие государства приветствуют Бельгию в качестве нового члена CRI.

На втором саммите CRI участники вновь подтвердили нашу совместную приверженность повышению нашей коллективной устойчивости к программам-вымогателям, сотрудничеству в борьбе с программами-вымогателями и преследованию виновных лиц, борьбе с незаконным финансированием, лежащим в

основе экосистемы программ-вымогателей, работе с частным сектором для защиты от атак программ-вымогателей. и продолжая международное сотрудничество по всем элементам угрозы программ-вымогателей.

Работа CRI поддерживает реализацию одобренной ООН концепции ответственного поведения государств в киберпространстве, в частности добровольной нормы о том, что государства должны сотрудничать «для обмена информацией, оказания помощи друг другу, судебного преследования за использование ИКТ террористами и преступниками и осуществления других совместных мер для устранить такие угрозы». Совместные усилия партнеров CRI также вносят непосредственный вклад в реализацию согласованных выводов и рекомендаций Группы экспертов ООН по проведению комплексного исследования киберпреступности.

Мы полны решимости использовать все соответствующие инструменты национальной власти для достижения этих целей и вместе привержены следующим действиям в поддержку этого усилия. Мы намерены:

Привлекать к ответственности субъектов программ-вымогателей за их преступления и не предоставлять им безопасное убежище;

Бороться со способностью субъектов программ-вымогателей получать прибыль от незаконных доходов путем внедрения и обеспечения соблюдения мер по борьбе с отмыванием денег и противодействию финансированию терроризма (AML/CFT), включая правила «знай своего клиента» (KYC) для виртуальных активов и поставщиков услуг виртуальных активов.

Пресекать и привлекать к ответственности лиц, занимающихся программами-вымогателями, а также и их пособников в максимально возможной степени, разрешенной действующим законодательством каждого партнера и соответствующими органами.

Сотрудничать в борьбе с программами-вымогателями путем обмена информацией, где это уместно и в соответствии с применимыми законами и нормативными актами, о неправомерном использовании инфраструктуры для запуска атак программ-вымогателей, чтобы гарантировать, что национальная киберинфраструктура не используется в атаках программ-вымогателей.

Для повышения нашей устойчивости к атакам программ-вымогателей требуются эффективные политики и сотрудничество с надежными партнерами. Члены CRI создают сеть доверенных партнеров для обмена и распространения информации об угрозах, связанных с программами-вымогателями, чтобы повысить нашу коллективную устойчивость к атакам программ-вымогателей. С этой целью мы намерены создать добровольную Международную целевую группу по борьбе с программами-вымогателями (ICRTF) для разработки межотраслевых инструментов и обмена данными о киберугрозах для расширения возможностей раннего предупреждения и предотвращения атак, а также для консолидации политики и передовой практики. ICRTF планирует публиковать публичные отчеты об инструментах, тактиках и процедурах для повышения осведомленности заинтересованных сторон во всем мире, продвижения и поощрения членства в CRI и повсеместного улучшения кибергигиены.

Мы обязуемся внедрить процессы для наиболее эффективного обмена информацией и анализом конкретных штаммов программ-вымогателей на постоянной и постоянной основе, чтобы повысить нашу коллективную осведомленность и устойчивость.

Члены CRI обязуются принимать меры в соответствии с национальным законодательством и политикой, чтобы разрушить и ухудшить экосистему программ-вымогателей и привлечь к ответственности преступников, занимающихся программами-вымогателями, на основе наших коллективных знаний, опыта, полномочий и возможностей. Мы намерены улучшить наше всестороннее и целостное понимание стратегий, используемых этими преступными деятелями, и средств, с помощью которых их злонамеренная деятельность может быть идентифицирована и рассмотрена в соответствующих юрисдикциях, чтобы улучшить наши инструменты, соответствующие органы и возможности для нарушения. Мы обязуемся работать вместе, чтобы расставить приоритеты в целях подрыва, чтобы использовать широту полномочий и инструментов, доступных для более эффективного достижения сложных и сложных целей. Мы намерены увеличить количество и влияние наших деструктивных действий, чтобы деятели программ-вымогателей были остановлены на своем пути.

CRI стремится не только защищать себя и друг друга от программ-вымогателей, но и помогать другим странам защищать и разрушать, чтобы программы-вымогатели не могли получить распространение во всем мире. С этой целью мы намерены делиться технической информацией и информацией об угрозах, а также предоставлять рекомендации по защите и исправлению как можно более широко.

Принятие решительных мер по противодействию незаконному финансированию, которое часто способствует и поддерживает прибыльность программ-вымогателей, также будет ключом к нашему коллективному успеху. Мы полны решимости работать над созданием механизмов для уведомления финансовых учреждений и платформ виртуальных активов о платежах программ-вымогателей, чтобы средства могли быть конфискованы после того, как они попадут на счета злоумышленников-вымогателей. Мы обязуемся работать вместе над продвижением средств контроля ПОД/ФТ, включая политики и процедуры KYC в рамках экосистемы виртуальных активов, чтобы предотвратить их использование для программ-вымогателей, например, путем реализации и обеспечения соблюдения рекомендаций Группы разработки финансовых мер борьбы с отмыванием денег.

Частный сектор играет уникальную роль в наших усилиях по борьбе с программами-вымогателями, поскольку их информация о местонахождении и действиях субъектов программ-вымогателей из Интернета может эффективно дополнять возможности государства в этой области. Компании частного сектора часто становятся жертвами программ-вымогателей и могут быть сильными союзниками в защите и разрушении. Члены CRI тесно сотрудничают с частным сектором, чтобы обмениваться информацией и ставить цели по предотвращению, сокращению и реагированию на угрозы программ-вымогателей. Для дальнейшего развития этого сотрудничества мы создали пилотную платформу для обмена информацией, чтобы облегчить обмен информацией об участниках и инструментах

программ-вымогателей, тактиках, методах и процедурах между участниками и, в конечном итоге, с частным сектором. Кроме того, мы также намерены разработать инструмент для наращивания потенциала, чтобы помочь странам использовать государственно-частные партнерства для борьбы с программами-вымогателями. Мы продолжаем совместную работу по разработке дополнительных способов сотрудничества в борьбе с программами-вымогателями с частным сектором, принимая во внимание опасения, которые могут возникнуть у компаний частного сектора.

Дипломатическое взаимодействие продолжает оставаться важным инструментом в борьбе международного сообщества с атаками программ-вымогателей. Мы полны решимости продолжать совместную работу не только в качестве CRI, но и с другими партнерами, приверженными борьбе с программами-вымогателями, которые могут повлиять на всех нас, в том числе в рамках Парижского призыва к доверию и безопасности для членов CRI, которые поддерживают звонок. Члены CRI планируют работать со всем спектром заинтересованных сторон, чтобы стимулировать целенаправленные региональные усилия и продвигать эту повестку дня в соответствующих многосторонних рамках, чтобы обеспечить общую решимость и готовность мирового сообщества противостоять этим угрозам. Мы также привержены использованию программ наращивания потенциала для повышения устойчивости, улучшения возможностей для разрушения, расширения возможностей правоохранительных органов, и поддерживать разработку правовой базы для борьбы с программами-вымогателями как в ЧРИ, так и в других странах. В связи с этим мы намерены проводить два раза в год киберучения для государств-членов CRI, которые также будут способствовать активизации инструментария ICRTF». ***(International Counter Ransomware Initiative 2022 Joint Statement // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/cybersecurity-professionals-may-be-burning-out-at-a-faster-rate-than-frontline-healthcare-workers/). 02.11.2022).***

***

«На прошлой неделе состоялся второй саммит Международной инициативы по борьбе с программами-вымогателями, в котором приняли участие лидеры из более чем 30 стран на первой личной встрече такого рода, чтобы обсудить глобальный ответ на угрозу атак программ-вымогателей. На саммите в Белом доме среди прочих мер обсуждалась разработка международной платформы для обмена информацией, стандартизированного инструментария для расследований и целевой группы.

На втором саммите Белого дома по программам-вымогателям представлен широкий спектр предложений

В то время как первый саммит в Белом доме был встречей в Zoom, которую некоторые критиковали за то, что она не содержала ничего, кроме «банальности», недавнее мероприятие завершилось широким спектром предложений по борьбе с атаками программ-вымогателей.

Одним из таких элементов является Международная целевая группа по борьбе с программами-вымогателями (ICRTF), которая предоставит членам центральную

систему, с помощью которой можно обмениваться возможностями и информацией с целью пресечения и отслеживания незаконной финансовой деятельности. Создание комбинированной ячейки в Региональном центре киберзащиты (RCDC) в Литве будет масштабной тестовой версией концепции, при этом Литва, возможно, была выбрана из-за близости к Калининградской области России и прямого знакомства с неистовыми бандами вымогателей в этом районе. Эта организация также будет публиковать полугодовой публичный отчет о тенденциях в атаках программ-вымогателей и предлагаемых мерах по смягчению последствий.

Что касается России, то страна участвовала в саммите в прошлом году, но не была приглашена на этот саммит. Том Келлерманн, CISM, старший вице-президент по киберстратегии в Contrast Security, который работал в Комиссии по кибербезопасности администрации президента Барака Обамы, которая работала над оценкой и улучшением киберинфраструктуры США, указал, что это, вероятно, связано не только с ситуацией на Украине, но и с возможными планами дальнейших санкций, связанных с атаками программ-вымогателей, которые исходят из страны: «Большинство атак программ-вымогателей осуществляется русскоязычными картелями, у которых есть Pax Mafioso с российским режимом. Они не только компенсируют экономические санкции, но и действуют как киберополченцы против западных целей в периоды геополитической напряженности. Мы должны расширить законы о конфискации, чтобы разрешить более масштабные аресты активов, которыми владеют киберпреступники. Кроме того, любая биржа, которая не охватывает арендаторов Группы разработки финансовых мер борьбы с отмыванием денег (FATF) и явно участвует в отмывании доходов от киберпреступлений, должна быть закрыта с помощью киберсредств, а их активы конфискованы и использованы для защиты критической инфраструктуры. Наконец, страховщикам следует запретить осуществлять платежи программ-вымогателей, поскольку эти платежи нарушают санкции, наложенные на Россию и Северную Корею».

Еще одним предложением саммита Белого дома является стандартизированный «инструментарий следователя» для глобального использования в ответ на атаки программ-вымогателей со стороны крупнейших преступных группировок мира. Это может включать публикацию досье о тактике, методах и процедурах для этих организаций, которые будут доступны для общественности.

Саммит в Белом доме также призвал к расширению сотрудничества между международными правоохранительными органами в борьбе с «тяжелыми и сложными целями». Это может включать в себя учебные мероприятия, такие как проводимые два раза в год учения по противодействию программам-вымогателям, семинар по противодействию программам-вымогателям по борьбе с незаконным финансированием (аналогичный семинару, который уже проводился Министерством финансов США в июле этого года), а также согласование рамок и руководящих принципов, которые будут использоваться в делах между юрисдикциями.

Саммит в Белом доме дополнительно ввел меры по зацикливанию частного бизнеса, где это применимо. Были разговоры об «инструменте наращивания потенциала», который объединил бы тематические исследования предыдущих атак

программ-вымогателей, в которых участвовали государственно-частные партнерства. «Расширение участия частного сектора» также было указано в качестве ключевой задачи на предстоящий год, хотя и без особой конкретики. На саммит были приглашены 13 международных компаний частного сектора (в том числе Microsoft, Siemens и ряд ведущих фирм в области кибербезопасности), и их спросили, что они в настоящее время делают в отношении атак программ-вымогателей и что, по их мнению, правительство должно делать в партнерстве с ними.

Джефф Уильямс, соучредитель и технический директор Contrast Security, поделился некоторыми мыслями о том, как могут выглядеть эти государственно-частные усилия в будущем: «Я понимаю, что отрасль и СМИ стали слишком осведомлены о программах-вымогателях и подобных атаках, но я думаю областью внимания, которая должна быть более приоритетной, является растущее количество атак нулевого дня и уязвимостей CVE. Программа-вымогатель обычно является результатом использования злоумышленником уязвимостей, таких как известные CVE. Из-за этого нам нужно сосредоточиться на основных причинах программ-вымогателей и других типов нарушений. Я думаю, что нам нужно сильное государственно-частное партнерство, чтобы сосредоточиться на прозрачности кибербезопасности, особенно в процессах разработки программного обеспечения и цепочки поставок. Нам нужно гораздо больше информации о том, как защищено программное обеспечение, которому мы доверяем самые важные вещи в нашей жизни. И нам необходимо работать над устранением целых классов уязвимостей из наших программных сред за счет улучшения защиты программного обеспечения и использования таких технологий, как самозащита приложений во время выполнения (RASP). Кроме того, мы должны дать отпор отрасли, когда она пытается запутать видимость слабых методов и технологий безопасности, утверждая, что это поставит под угрозу интеллектуальную собственность (это не будет) или упростит задачу для злоумышленников (это не так)».

Участники саммита в Белом доме также договорились в принципе увеличить как дипломатические усилия, так и «политические издержки» для стран, которые укрывают цифровые преступные группировки и позволяют запускать атаки программ-вымогателей изнутри своих границ, что может стать еще одним ударом по России.

Саммит в Белом доме может привести к активным действиям по борьбе с атаками программ-вымогателей в следующем году

Саммит в Белом доме был закрыт для средств массовой информации, за исключением заключительного заседания, поэтому подробности остаются скудными, если не считать выпущенных пресс-релизов. Однако планы предложений амбициозны и могут привести к значительным действиям в краткосрочной перспективе по сдерживанию атак программ-вымогателей, если они продолжатся.

Администрация ясно видит необходимость немедленных действий, ссылаясь на широко распространенные атаки программ-вымогателей на школы и больничные сети по всему миру. Поток незаконной криптовалюты, по-видимому, является еще одним важным направлением: высокопоставленный представитель администрации рекламирует санкции администрации в отношении Tornado Cash и указывает, что

Целевая группа по финансовым мероприятиям Министерства финансов США стремится внедрить правила «Знай своего клиента» для торговли криптовалютой.

Однако еще предстоит увидеть, что на самом деле выйдет из саммита в Белом доме. Также было достигнуто общее принципиальное соглашение о разработке централизованной международной системы обмена информацией и принятии более строгих мер против отмывания денег с использованием криптовалюты, но практически никаких последствий не произошло; совместные международные усилия все еще находятся на стадии планирования, и санкция Tornado Cash не была получена до тех пор, пока не было обнаружено, что хакеры, поддерживаемые государством Северной Кореи, активно атаковали блокчейн-мосты и использовали сервис для отмывания своих украденных токенов.

Полезных новостей для частного бизнеса было немного, но Эрих Крон (адвокат по вопросам безопасности в KnowBe4) предлагает несколько общих рекомендаций для тех, кто все еще хочет улучшить свою защиту: «Пока мы не сможем придумать решение проблемы, организациям следует сосредоточиться на снижении риска заражения, сосредоточив внимание на ключевых путях распространения программ-вымогателей, фишинговых атаки и порталы удаленного доступа. Обучение сотрудников навыкам быстрого и точного обнаружения фишинговых атак и сообщения о них, а также обеспечение безопасности порталов удаленного доступа с помощью многофакторной аутентификации (MFA) может значительно снизить вероятность первоначального заражения. Устранение уязвимостей программного обеспечения и сегментация сетей могут ограничить возможность распространения вредоносного ПО в организации, а надежные средства защиты от потери данных (DLP) могут уменьшить угрозу утечки данных, лишив злоумышленников ключевого рычага воздействия». ***(Scott Ikeda. White House Summit on Ransomware Attacks Brings Global Leaders Together To Discuss Information Sharing, Defense Frameworks // CPO Magazine (https://www.cpomagazine.com/cyber-security/white-house-summit-on-ransomware-attacks-brings-global-leaders-together-to-discuss-information-sharing-defense-frameworks/). 08.11.2022).***

***

«Компания признала атаку в августе и с тех пор молчит о хакерах

Группа вымогателей LockBit берет на себя ответственность за атаку на немецкого производителя автозапчастей Continental, поскольку она угрожает утечкой данных компании.

Группа добавила Continental - производителя шин, тормозных систем и внутренней электроники стоимостью 33,8 миллиарда евро - к своему сайту утечки в четверг, дав компании крайний срок в пятницу, чтобы отреагировать на ее требование о вымогательстве.

В августе транснациональная корпорация из Ганновера признала, что столкнулась с кибер-инцидентом, но заявила, что отпугнула хакеров. «Компания сохраняет полный контроль над своими ИТ-системами», — говорится в сообщении.

С тех пор Continental не предоставила обновленную информацию и не предоставила дополнительную информацию при обращении.

LockBit стала ведущей группой после Conti, предлагающей программы-вымогатели как услугу, или, по крайней мере, ее постоянная самореклама побуждает людей так думать (см. Ключи к успеху LockBit: самореклама, техническая хватка). Основываясь на мониторинге мест утечек, Malwarebytes постоянно ставит LockBit на первое место в своем списке наиболее активных групп программ-вымогателей. Сайты утечек имеют хорошо известные предубеждения для определения активности программ-вымогателей, но являются источником данных в ландшафте, в противном случае лишенном этого.

Группа получила широкую огласку в СМИ, когда в июне объявила о программе вознаграждения за обнаружение ошибок. В сентябре группа заявила, что в сентябре она произвела платеж в размере 50 000 долларов.

В июне он выпустил версию 3.0 своего вымогателя. Просочился его билдер, возможно, бывшим разработчиком LockBit. Создатель, по-видимому, предлагает «высокий уровень настройки», пишет Malwarebytes, отмечая, что хакеры, выполняющие грязную работу по установке LockBit на компьютеры жертв, «могут выбрать свой собственный C2-сервер, выбрать процессы, которые они хотят завершить, изменить записку о выкупе, и так далее». ***(Akshaya Asokan. LockBit Claims Attack on German Auto Parts Giant Continental // Information Security Media Group, Corp. (https://www.govinfosecurity.com/lockbit-claims-attack-on-german-auto-parts-giant-continental-a-20418). 04.11.2022).***

***

«Жестокие последствия невыплаты выкупа банде кибер-вымогателей стали болезненно очевидными в Австралии на этой неделе.

Во вторник группа программ-вымогателей начала публиковать некоторые данные, украденные из систем Medibank, одной из крупнейших страховых компаний Австралии. Накануне Medibank публично объявил, что не будет платить выкуп. (см.: Medibank отказывается платить хакерам за вымогательство).

Medibank сообщает, что нарушение затронуло 9,7 миллиона нынешних и бывших клиентов. Данные включают информацию, связанную с претензиями, в том числе коды медицинских диагнозов, например, курит ли человек или может ли он употреблять запрещенные наркотики.

В четверг банда вымогателей заявила, что хочет 10 миллионов долларов США — 15 миллионов австралийских долларов — за то, чтобы не публиковать данные, но сказала, что она сократится до 9,7 миллиона долларов, что равняется 1 доллару за каждую запись. Он также опубликовал очень конфиденциальный файл записей страхователей, который содержал медицинские коды, связанные с абортом.

Это заставило некоторых задаться вопросом, стоило ли платить выкуп и не следовало ли использовать инцидент с Medibank, чтобы привлечь внимание киберпреступного мира. Однако оплата противоречила бы совету правительства Австралии.

Сдерживание нарабатывается со временем и не сформируется в результате реакции на один инцидент. Учитывая характер данных, этот выделяется. И выбор не платить тоже. Это действительно посылает сообщение, но оно болезненно затрагивает 9,7 миллиона человек.

Medibank считает премьер-министра страны и, по иронии судьбы, ее министра кибербезопасности клиентами. Утечка данных и последующее вымогательство заставили страну серьезно задуматься о том, достаточно ли сильны ее законы для защиты личных данных.

Министр внутренних дел и кибербезопасности Клэр О'Нил заявила парламенту в среду: «Я не могу выразить свое отвращение к отморозкам, которые стоят за этим преступным деянием. Люди имеют право хранить информацию о своем здоровье в тайне».

«Даже среди атакующих программ-вымогателей идея раскрытия личной медицинской информации других людей считается запредельной. Так что не заблуждайтесь: это не просто обычная группа подлых преступников. Это низший из низших».

Medibank заявил, что скомпрометированные учетные данные для входа привели к утечке данных. Чтобы было ясно, мы до сих пор точно не знаем, как эти украденные учетные данные для входа привели к потере личных данных 9,7 миллиона человек.

Но злоумышленники раскрыли некоторые детали в своем первом пакете данных, который включал в себя журналы разговоров, которые они вели с официальными лицами Medibank.

В чате есть комментарий, который указывает на то, что злоумышленники имеют доступ к VPN. Затем злоумышленники утверждают, что они получили доступ к Redshift, продукту хранилища данных Amazon, через серверы перехода.

We accessed Redshift on jump servers.
And download the data in csv files with our application.
Then we uploaded the data to our server.
Guided by the source code and documentation from Confluence, we linked the data and made selections.
Here is the listing of the files: csv(data from redshift), confluence, stash (source code).
Based on confluence we've accessed all 7 layers including RedShift and Glue using a workbench. We'll spent about a month to figure out in your system and dump a tables with PII data.

В просочившемся журнале чата злоумышленники-вымогатели описали, как они проникли в системы Medibank.

Злоумышленники Medibank, которых некоторые исследователи называют BlogXX, заявили, что они потратили месяц на изучение систем медицинского страхования. В конце концов, они удалили таблицы базы данных SQL, содержащие информацию, позволяющую установить личность, и поместили эти данные в файлы.csv, которые они предоставили Medibank в качестве доказательства вторжения.

Злоумышленники также утверждают, что получили доступ к серверу Medibank Confluence, который является программным обеспечением Atlassian для совместной работы, и захватили исходный код из Stash, инструмента управления исходным кодом.

Скомпрометированные учетные данные доступа

Medibank в конце концов поймал злоумышленников, но только после того, как банда украла личные данные. В конце прошлого месяца Medibank заявил, что обнаружил предшественников атаки программ-вымогателей и считал, что доступ к данным не был получен. Казалось бы, положительная история, но вскоре после этого

Medibank сообщил общественности, что злоумышленники на самом деле украли данные и связались с ними, желая договориться.

Как злоумышленники получили украденные учетные данные для доступа? Недавно я разговаривал с бывшим сотрудником Medibank, чьи учетные данные для входа появились в даркнете в августе, и завязался интересный разговор.

Для фона учетные данные для входа постоянно крадут, покупают и продают. «У каждой организации есть кредиты на продажу», — говорит мне один источник. Медибанк ничем не отличается. По данным лос-анджелесской аналитической компании Resecurity, специализирующейся на кибербезопасности, в августе было доступно для продажи не менее полдюжины счетов Medibank.

Я посмотрел учетные данные и написал некоторым людям по электронной почте. Один откликнулся, и мы поговорили по телефону. Он был сотрудником службы поддержки COVID в Medibank на полставки. Страхователи звонили с вопросами о COVID, и он сказал, что прочитает руководство по COVID на веб-сайте Нового Южного Уэльса.

Его адрес электронной почты и пароль Medibank продавались вместе с URL-адресом, где эти учетные данные были действительными. Его данные были собраны вредоносным ПО ботнета Redline, которое, по-видимому, заразило одно из его устройств.

Но он говорит, что не верит в это, поскольку использует четыре антивирусных программы и осторожен с потенциально вредоносными ссылками. Его банковский счет в ANZ был заблокирован после того, как хакеры также преследовали его в августе, но он не потерял деньги.

Он работал из дома и входил в системы Medibank, используя свой адрес электронной почты и пароль. Затем он вводил одноразовый пароль из генератора VIP-кода Symantec на своем телефоне. Оказавшись внутри, он получил доступ к порталу потока пациентов Medibank.

Он мог видеть имена, адреса, местный медицинский округ, в котором живет человек, а иногда и информацию о заболевании, связанную с COVID. Но он говорит, что был «предел» того, к какой информации о пациентах он мог получить доступ.

Он покинул Medibank в мае, поэтому, если Medibank следовал передовым методам ИТ-безопасности, его учетные данные для входа должны были быть отозваны тогда. Здорово, что у Medibank есть двухфакторная аутентификация, но есть разные хитрости, чтобы обойти это.

Привел ли взлом аккаунта этого человека к тому состоянию, в котором сейчас находится Medibank? Наверное, нет, но это тоже не исключено. Реагирование на инциденты Medibank и судебно-медицинское расследование могут выяснить, с чего все это началось и была ли это эта учетная запись или другая.

Но вместо того, чтобы пытаться спекулировать на том, кто является «нулевым пациентом», эта история предназначена для того, чтобы показать возможный вредоносный путь через украденные учетные данные: вредоносное ПО на рабочем компьютере > собранные учетные данные для входа > доступ к корпоративной сети > другие коварные вещи, в зависимости от того, какие меры безопасности установлены. И затем, в конце концов, возможно, самая серьезная утечка данных в истории Австралии». ***(Jeremy Kirk. Australia Faces Consequences of Standing Up to***

Ransomware // Information Security Media Group, Corp. (https://www.govinfosecurity.com/blogs/australia-faces-consequences-standing-up-to-ransomware-p-3312). 10.11.2022).

***

«Группа вымогателей дала Medibank 24 часа на оплату. Но Medibank говорит, что этого не будет.

Кто пытается вымогать деньги у австралийской страховой компании Medibank? Почему Medibank сказал злоумышленникам, что не будет платить выкуп? Отпугнет ли это будущих кибер-вымогателей? Вот несколько мыслей о разыгравшейся драме о киберпреступности.

В понедельник Medibank публично заявил, что не будет платить выкуп злоумышленникам, которые, по его словам, получили конфиденциальные данные о 9,7 миллионах текущих и бывших клиентов. Сегодня этот гамбит вызвал реакцию: 24-часовой крайний срок, чтобы заплатить или увидеть раскрытие конфиденциальных данных о медицинских требованиях (см.: Medibank говорит «нет» платежному требованию хакера о вымогательстве).

Заявление Medibank было эквивалентно подбрасыванию птицы злоумышленникам, и оно согласуется с позицией правительства Австралии. Генеральный директор Medibank Дэвид Кочкар сказал, что сумма, запрошенная вымогателями, которую он не раскрыл, «не имеет значения». По его словам, даже если Medibank заплатит, нет гарантии, что данные будут удалены. Он прав.

Что примечательно и почти неслыханно, так это то, насколько открытым и прозрачным был Medibank на каждом шагу в этой чрезвычайно сложной ситуации. Публично заявить, что выкуп не будет выплачен, было поразительно смелым шагом. Редко компании говорят так или иначе, если они заплатили.

Вымогатели: BlogXX

Группа вымогателей сделала предупреждение Medibank в своем блоге на.onionсайте. Некоторые исследователи киберпреступности назвали группу «BlogXX», поскольку у нее нет четкого названия.

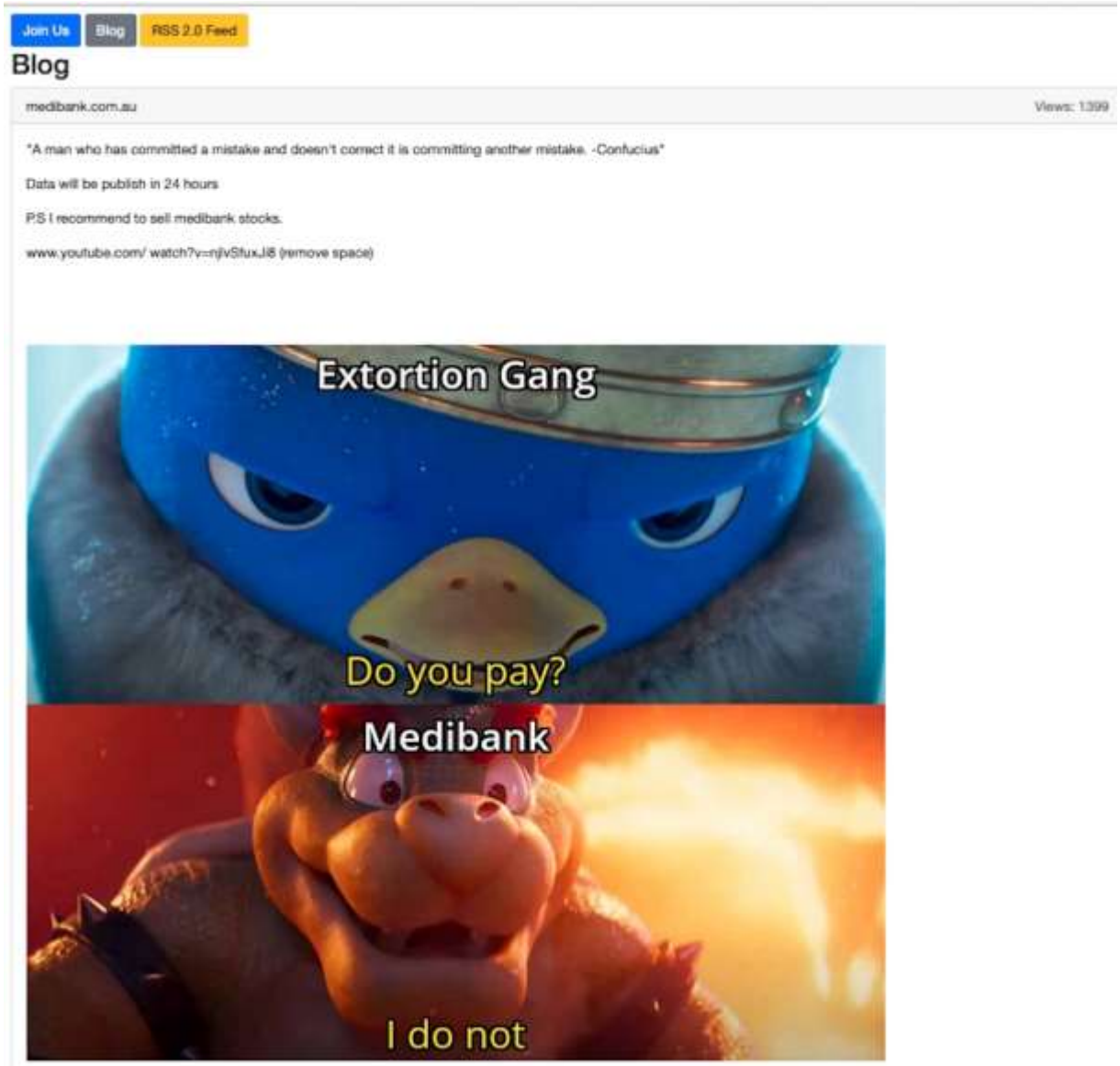
Веб-сайт BlogXX содержит ссылки на печально известную банду вымогателей REvil, которая атаковала разработчика программного обеспечения Kaseya в июле 2021 года и JBS Foods в мае 2021 года. Оба инцидента имели серьезные последствия в Австралии.

Банды REvil больше нет, и ее упадок читается как роман о киберпреступности мафии: вымогательство, куча денег, предательство, аресты в России и падение группы примерно в октябре 2021 года.

Но внезапно в апреле часть старой инфраструктуры REvil, которая использовалась для утечки данных, начала перенаправляться на веб-.onionсайт BlogXX, согласно Bleeping Computer.

BlogXX считается группой вымогателей, а не чистой группой вымогателей, поскольку когда-то она использовала вариант вредоносного ПО REvil для шифрования файлов. Medibank заявил вскоре после того, как впервые публично объявил об инциденте, что остановил «предшественников» атаки программ-вымогателей.

BlogXX предупредил в своем последнем посте, что «данные Medibank будут опубликованы в течение 24 часов» и «PS я рекомендую продать акции medibank». Он также связан с видео на YouTube с недавним сатирическим произведением австралийского комика Марка Хамфриса о Medibank. Образца данных нет, но, учитывая историю веб-сайта, это, вероятно, реальная угроза.



Группа вымогателей, которую некоторые исследователи киберпреступности называют BlogXX, угрожает раскрыть конфиденциальные данные, которые она украла у австралийской страховой компании Medibank.

Куда это идет отсюда? Данные, вероятно, начнут сбрасываться в течение дня или около того, если Medibank не изменит свою позицию по выплате выкупа, что маловероятно. Будет ли неплатеж посылать сообщение другим бандам вымогателей или вымогателей, чтобы они не связывались с Австралией? Они, без сомнения, примут к сведению.

Но киберпреступники не соблюдают нормального сдерживания. Атаки на ИТ-системы имеют низкую альтернативную стоимость. И, вероятно, есть довольно много австралийских компаний, которые платили выкуп на протяжении многих лет. Как это вытряхивается? Потребуется гораздо больше компаний, чем просто

Medibank, сказавший «нет» вымогательству. Но это отличное начало». ***(Jeremy Kirk. Who Is Extorting Australian Health Insurer Medibank? // Information Security Media Group, Corp. (https://www.govinfosecurity.com/blogs/who-extorting-australian-health-insurer-medibank-p-3310). 08.11.2022).***

***

«Программа-вымогатель остается самой большой онлайн-угрозой, предупреждает генеральный директор NCSC Линди КэмеронМэтью Дж. Шварц… По словам главы британского отдела кибербезопасности, подавляющее большинство атак программ-вымогателей можно было бы полностью заблокировать, если бы жертвы сосредоточились на основах кибербезопасности.

«Мы по-прежнему считаем, что 90% инцидентов в Великобритании можно было бы предотвратить, если бы люди следовали основам», — заявила Линди Кэмерон, президент Национального центра кибербезопасности Великобритании, участникам недавнего саммита по кибербезопасности в Шотландии.

Программа-вымогатель остается самой большой онлайн-угрозой, с которой сталкивается Великобритания, особенно сильно поражая больницы и школы, сказала Кэмерон, которая возглавляет NCSC, который является открытым подразделением британского агентства безопасности, разведки и кибербезопасности, GCHQ. В новом отчете NCSC предупреждает, что в ближайшие месяцы ожидается всплеск атак программ-вымогателей.

Как и правительство США, британское правительство не запрещает платить выкуп, если это не нарушает санкции. Тем не менее, «наш стандартный совет: не делайте этого», — сказала Кэмерон участникам саммита CyberScotland 27 октября, состоявшегося в отеле Balmoral в Эдинбурге. «Как только вы заплатите, гораздо больше шансов снова сделать вас жертвой».

Оплата также побуждает существующих преступников продолжать и привлекает новых участников. Конечно, иногда оплата является единственным вариантом, доступным для организации, которая в противном случае могла бы обанкротиться, сказала Кэмерон, и «действительно важно не подвергать жертв повторной виктимизации».

Кэмерон сказала, что, чтобы помочь избежать нормализации этой практики или сделать Великобританию легкой мишенью, любой, кто рассматривает возможность уплаты выкупа, должен относиться к этому так, как будто он стоит на углу улицы и передает огромный мешок с деньгами известному преступнику. «Вы должны чувствовать себя довольно некомфортно», — сказала она.

Упражнение в коробке

Как организации могут лучше подготовиться к отражению и смягчению последствий онлайн-атак? Кэмерон призвала организации использовать бесплатный онлайн-инструмент «Упражнение в коробке» NCSC, чтобы помочь определить, насколько они устойчивы к онлайн-атакам, а также спроектировать и разработать более эффективные планы реагирования на инциденты.

По словам генерального директора Scottish Business Resilience Center Джуда Маккорри, это упражнение должно быть легко доступным. «Это всего лишь полтора часа. Это бесплатно. Пойдем», — сказала она.

Согласно SBRC, инструмент представляет собой «коробку, полную упражнений, основанных на реальных сценариях, с наводящими вопросами, прикрепленными к каждому сценарию. Он позволяет вашей организации выполнять их в удобное время, в безопасной среде столько раз, сколько вы хотите».

Кэмерон из NCSC говорит, что инструмент был запущен не только в Великобритании, но и за рубежом, в том числе совсем недавно в Сингапуре. «Справедливости ради следует отметить, что мы сами запустили его как совет GCHQ, и он многому нас научил. Независимо от того, как много вы знаете о кибербезопасности, вы всегда можете узнать больше о реакции вашей организации», — сказала она. «Например, часто те части организации, которые думают, что их работа не связана с кибербезопасностью, могут сделать больше, поэтому команда связи… человеческие ресурсы», а также все, кто поддерживает связь с клиентами, поставщиками и деловыми партнерами.

Кэмерон сказала, что это упражнение «демистифицирует» лучшее понимание кибербезопасности и планирование реагирования, добавив, что «они объединяют [людей] и дают им общий язык». Она также сказала: «Я действительно хочу убедиться, что мы не позволим старшим руководителям сорваться с крючка».

Некоторые участники — в основном профессионалы в области кибербезопасности — сказали, что общей проблемой остается заставить организацию говорить о безопасности. Один из присутствующих директоров по информационной безопасности сказал, что высшее руководство увеличило бюджет безопасности в пять раз после того, как их организация пострадала от атаки программы-вымогателя, которая, к счастью, вывела из строя лишь несколько компьютеров.

Учимся на прошлых инцидентах

Как подчеркивали выступающие на саммите, устойчивость к инцидентам и планирование реагирования остаются постоянной практикой.

Одним из эталонных инцидентов кибербезопасности, о которых упоминалось в течение дня, была атака программ-вымогателей в канун Рождества 2020 года на Шотландское агентство по охране окружающей среды (см. Реагирование после программ-вымогателей: жертва говорит: «Делай правильно»).

SEPA стала жертвой атаки, несмотря на надежную защиту. «SEPA не является и не была плохо защищенной организацией», — заявил Малкольм Грэм, заместитель начальника полиции Шотландии, в 2021 году во время реагирования на инцидент.

Агентство отказалось платить выкуп. В ответ злоумышленник — часть операции Conti по программе «вымогатель как услуга» — слил украденные данные.

Работая с полицией и SBRC, SEPA начала долгосрочную работу по реагированию на инциденты, которая включала перестройку многочисленных систем, чтобы сделать их более устойчивыми, несмотря на связанные с этим усилия и затраты.

Инцидент побудил официальных лиц задаться вопросом: «Есть ли у Шотландии возможность управлять несколькими инцидентами одновременно?» Об этом участникам саммита заявила глава отдела киберустойчивости правительства Шотландии Клэр Эль-Азебби.

Теперь ответ, говорит она, «да». Но в то время, когда был нанесен удар по SEPA, ответ был бы «нет», и если бы произошло более одного одновременного инцидента, это было бы «катастрофой для страны», сказала она.

Обрезание кабеля подчеркивает киберриски

Несколько выступавших заявили, что устойчивость заключается не в том, чтобы быть идеальным, а в том, чтобы попытаться обеспечить организации надежными планами для покрытия различных типов инцидентов хорошо отработанным и скоординированным образом.

Менее трех недель назад связь между материковой Шотландией и островом Шетланд прервалась после того, как рыболовецкий траулер случайно перерезал подводный кабель. Хотя этот инцидент не был связан с какой-либо онлайн-атакой, он подчеркнул влияние, которое внешние события могут оказать на критически важные ресурсы, которые могут стать мишенью для преступников и нападающих на национальное государство, сказал MSP Кит Браун, секретарь кабинета министров Шотландии по вопросам юстиции и безопасности. Ветераны в своем вступительном слове.

Проблема усугублялась совпадением, что случается часто. В этом случае подводный кабель от Шетландских островов до Фарерских островов был остановлен на техническое обслуживание.

В результате обрыв кабеля «не означал полного отключения связи, но большинство людей не могли использовать технологии мобильных телефонов или другие средства связи, основанные на кабеле», — сказал он. Это означало, что банки не могли выдавать наличные, за исключением одного, который это делал, используя рукописные бухгалтерские книги; магазины не могли продавать продукты питания; и общественность запаниковала.

«Очень плохих ситуаций никогда не было, но было совершенно очевидно, как быстро инцидент, связанный с кибербезопасностью, может иметь последствия второго и третьего порядка», — сказал Браун.

Это сообщение снова было перехвачено ФБР. «Киберриск — это бизнес-риск, а кибербезопасность — это бизнес-безопасность», — это сообщение бюро пытается донести до всех организаций, — сказал Дженсен Пеналоса, помощник атташе по правовым вопросам ФБР в Лондоне.

Как использовать анализ угроз

Многие организации полагаются на информацию об угрозах, чтобы отточить свои усилия в области кибербезопасности. Во время панельной сессии под названием «Подход к кибербезопасности на основе аналитики» Крис Уллиотт, директор по информационной безопасности NatWest Group, подчеркнул, что аналитика угроз должна быть дополнением к хорошо выполненным основам.

«Из разведданных, которые мы получаем, я знаю, что северокорейцы тратят много времени, пытаясь скомпрометировать финансовые учреждения, и, зная это, я могу посмотреть, как они работают и какие инструменты они используют, и это расставит для меня приоритеты в работе, которую я делаю», он сказал. Но это происходит после того, как я освоил основы, включая установку исправлений и многофакторную аутентификацию, «потому что, если я попытаюсь сделать все, я сделаю это плохо, и у меня все еще будут проблемы».

Модератор дискуссии, детектив-инспектор Норман Стивенсон из полиции Шотландии, спросил участников дискуссии, как они справляются с задачей формирования и сосредоточения разведывательных данных.

«Разведка должна быть действенной», — сказал Дон Смит, вице-президент по исследованию угроз в Secureworks, где он возглавляет разведывательную группу из 40 человек.

Он привел пример: «Если я взгляну на 79 операций с программами-вымогателями после вторжений, проведенных Secureworks в этом году до конца июля, для начального вектора заражения, 52% из них были злоумышленниками, которые могли сканировать и использовать неисправленные системы с выходом в Интернет», - он сказал. «Итак, есть бесплатная полезная информация: исправьте свои вещи».

Знать, какому интеллекту отдать предпочтение, — проблема. «Одной из самых больших проблем, с которыми мы сталкиваемся как банк, является фильтрация всех различных источников информации», — сказал Уллиотт из NatWest Group. «Нам нужно добраться до точки, когда разведданные будут более высокого качества. Так что, может быть, чем меньше, тем лучше, а наличие надежных партнеров высокого уровня может быть лучше».

Смит из Secureworks сказал, что для сбора информации он всегда спрашивает: что является источником и как он был собран? Это потому, что некоторые источники и методы лучше других, говорит он.

Кроме того, он спрашивает: есть ли у него временная метка, и если да, то «когда оно было опубликовано или когда за ним наблюдали?» Он сказал: «Если вы используете этот простой, грубый тест, вы можете выбросить 90% каналов, потому что большинство из них — мусор».

Другой тип разведки касается программ-вымогателей. Пеналоса из ФБР сказала, что один из способов, которым бюро работало над снижением воздействия программ-вымогателей, заключался в том, чтобы по возможности передавать разведывательные данные жертвам. В недавнем случае, например, она сказала, что жертва не была уверена, должна ли она платить выкуп, чтобы избежать утечки украденных данных, чего Кэмерон из NCSC и другие призвали их никогда не делать, поскольку большинство преступников могут продать данные в любом случае.

Чтобы проинформировать жертву о принятии решения, «мы смогли сообщить им, что злоумышленник, основываясь на… 14 предыдущих инцидентах, не обнародовали никаких данных», — сказала она. «Мы не сказали им, платить или нет… Мы не собираемся повторно виктимизировать жертву и мешать им выздоравливать». Но разведка помогла организации избежать выплаты сотен тысяч долларов преступникам». ***(Mathew J. Schwartz. Basics Will Block Most Ransomware Hits, Says UK Cyber Chief // Information Security Media Group, Corp. (https://www.govinfosecurity.com/basics-will-block-most-ransomware-hits-says-uk-cyber-chief-a-20426). 07.11.2022).***

***

«Проанализированные варианты программ-вымогателей — с июля по декабрь 2021 года — нанесли ущерб в миллионы долларов.

Новый анализ Сети по борьбе с финансовыми преступлениями Министерства юстиции показывает, что российские субъекты составили примерно три четверти зарегистрированных инцидентов с программами-вымогателями во второй половине 2021 года, что способствовало резкому росту атак программ-вымогателей в течение 2021 года по сравнению с 2020 годом.

Опираясь на данные, собранные в соответствии с Законом о банковской тайне и более ранним отчетом агентства, официальные лица FinCEN приписали 594 действия, связанных с программами-вымогателями, зарегистрированными в период с июля по декабрь 2021 года, субъектам, связанным с Россией, из кумулятивных 793 действий, о которых было сообщено агентству за это время. Рамка. Общая стоимость инцидентов за этот период времени составила 488 миллионов долларов.

«Сегодняшний отчет напоминает нам о том, что программы-вымогатели, в том числе атаки, совершаемые субъектами, связанными с Россией, остаются серьезной угрозой для нашей национальной и экономической безопасности», — сказал исполняющий обязанности директора FinCEN Химаули Дас. «Это также подчеркивает важность регистрации BSA, которая позволяет нам выявлять тенденции и закономерности в поддержку общегосударственных усилий по предотвращению атак программ-вымогателей и борьбе с ними. Финансовые учреждения играют решающую роль в защите Соединенных Штатов от угроз, связанных с программами-вымогателями, просто выполняя свои обязательства по соблюдению BSA».

Ранее в октябре FinCEN опубликовала более крупный отчет, в котором показано, что сумма денег, потерянных в результате атак программ-вымогателей, увеличилась с 527 миллионов долларов, потерянных в 2020 году, до примерно 886 миллионов долларов в течение 2021 года, что представляет собой увеличение стоимости вредоносных кибератак на 68%.

В частности, официальные лица зафиксировали 1251 атаку программ-вымогателей в 2021 году по сравнению с 602 инцидентами в 2020 году.

Этот новый отчет был посвящен вариантам программ-вымогателей или отдельным версиям программ-вымогателей, а также тому, насколько широко российские субъекты участвовали в развертывании вредоносного ПО. Авторы FinCEN рассмотрели 84 уникальных варианта программ-вымогателей за отчетный период в 2021 году и в конечном итоге определили, что около 58% из них связаны с подозреваемыми российскими кибер-злоумышленниками.

«Хотя атрибуция вредоносных программ затруднена, эти варианты были идентифицированы в информации из открытых источников как использующие русскоязычный код, закодированные специально для того, чтобы не атаковать цели в России или постсоветских государствах, или как реклама в основном на русскоязычных сайтах», — говорится в отчете. сказал.

Дальнейший анализ показал, что четыре из пяти самых дорогостоящих инцидентов с программами-вымогателями были связаны с Россией.

Отчет дебютирует, когда США участвуют во втором ежегодном саммите Международной инициативы по борьбе с программами-вымогателями, к которому присоединились еще 36 стран. Киберприсутствие России станет главной темой для обсуждения, поскольку вторжение страны в Украину вызвало геополитическую

напряженность и уступило место потенциальным спонсируемым Россией кибератакам на США и их союзников». ***(Alexandra Kelley. Russia Linked to Nearly 75% of Late 2021 Ransomware Attacks, Per Analysis // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/russia-linked-nearly-75-late-2021-ransomware-attacks-analysis/379197/). 01.11.2022).***

***

«После завершения инструмент будет содержать серию тематических исследований PPP, которые использовались в борьбе с программами-вымогателями.

Агентство по кибербезопасности и безопасности инфраструктуры (CISA) в партнерстве с Государственным департаментом США и Министерством внутренних дел Испании объявило на прошлой неделе о совместном проекте по разработке инструмента наращивания потенциала, который поможет странам использовать государственно-частные партнерства (ГЧП). для борьбы с программами-вымогателями. Этот проект был разработан в рамках Второго саммита Международной инициативы по борьбе с программами-вымогателями (CRI), который был созван в Вашингтоне, округ Колумбия. CRI — это глобальная коалиция 36 стран-партнеров и Европейского Союза, призванная противостоять угрозе программ-вымогателей.

Рабочая группа CRI по государственно-частному партнерству (P3) под председательством Испании сосредоточила внимание на необходимости тесного сотрудничества между правительствами и частным сектором для решения проблем, связанных с программами-вымогателями. Этот инструмент предоставит столь необходимое руководство странам всего мира, стремящимся развивать или углублять такие партнерства между государственным и частным секторами.

«Наращивание потенциала по всему миру — важный аспект нашей борьбы с программами-вымогателями, — сказал Брэндон Уэльс, исполнительный директор CISA. «Учась друг у друга — как в государственном, так и в частном секторе — и более широко делясь этими знаниями, мы можем эффективно защитить критически важную инфраструктуру, необходимую для поддержания не только американского общества, но и глобальных институтов и сетей, на которые оно опирается».

«Испания твердо убеждена, что этот проект внесет решающий вклад в демонстрацию самых передовых передовых методов ГЧП для борьбы с программами-вымогателями, — сказал Гильермо Ардизоне Гарсия, политический директор Министерства иностранных дел. «Таким образом, все заинтересованные стороны и партнеры, участвующие в CRI, получат выгоду от этого направления действий. Испания будет активно поощрять участие государственных и негосударственных заинтересованных сторон в этом проекте, чтобы широко делиться передовым опытом в области ГЧП, включая творческие схемы финансирования».

После завершения инструмент будет включать серию тематических исследований PPP, которые использовались в борьбе с программами-вымогателями, в том числе те, которые впервые были предложены членами рабочей группы CRI P3. Инструмент выделит особенности, которые сделали эти усилия успешными, и будет

разработан, чтобы предоставить практическое руководство странам, стремящимся внедрить свои собственные PPP в рамках своих национальных усилий по борьбе с программами-вымогателями.

Для разработки инструмента Соединенные Штаты и Испания сотрудничают с Глобальным форумом киберэкспертизы (GFCE), мировым лидером в области наращивания киберпотенциала, который поручит экспертам предоставить инструмент. Другим членам CRI было предложено оказать дополнительную финансовую и практическую поддержку проекту». ***(United States and Spain Announce the Development of a New Capacity Building Tool to Combat Ransomware // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/united-states-and-spain-announce-the-development-of-a-new-capacity-building-tool-to-combat-ransomware/). 11.11.2022).***

***

«Группа вымогателей Hive взяла на себя ответственность за кибератаку Tata Power и начала утечку украденных данных.

Tata Power признала кибератаку 14 октября в отчете фондовой биржи, заявив, что она извлекла и восстановила все системы.

«Компания предприняла шаги для извлечения и восстановления систем. Все критические операционные системы функционируют; однако в качестве меры предосторожности был введен ограниченный доступ и профилактические проверки для порталов и точек взаимодействия с сотрудниками и клиентами», — говорится в заявлении Tata Power.

Однако банда вымогателей Hive заявила, что зашифровала Tata Power 3 октября 2022 года, почти за две недели до того, как компания подала уведомление об утечке данных. Если это так, Tata Power рискует быть оштрафованным за нарушение правил Индийской группы реагирования на компьютерные чрезвычайные ситуации (CERT-In), которые требуют уведомления в течение шести часов после обнаружения.

Компания со штаб-квартирой в Мумбаи является частью конгломерата Tata Group, обслуживающей 12 миллионов клиентов, и является крупнейшей интегрированной энергетической компанией в стране.

Группа вымогателей Hive начала утечку украденных данных

Банда вымогателей Hive перечислила индийскую электроэнергетическую компанию на своем сайте утечки данных, предполагая, что переговоры о выкупе окончательно провалились.

Группа вымогателей также начала утечку украденных данных, включая конфиденциальную личную информацию, такую как номера национального удостоверения личности (Aadhar), налоговые идентификаторы (PAN), номера телефонов, домашние адреса и информацию о зарплате. Украденные данные также включали закрытые ключи, банковские и финансовые записи, клиентские контракты и технические чертежи.

По словам исследователя кибербезопасности Ракеша Кришнана, банда вымогателей слила не менее 20 банковских записей.

Эдвард Либих, глобальный директор кибер-экосистемы Hexagon Asset Lifecycle Intelligence, предупредил, что выплата выкупа не гарантирует восстановление украденных данных.

«Скажем прямо, даже если переговоры пройдут успешно, вероятность восстановления зашифрованных активов составляет всего 50% на 50%. Решение платить или не платить — дело деловое».

Однако он признал некоторые исключения, которые могут заставить компанию заплатить выкуп в надежде восстановить украденные данные.

«Если организация находится в очень уязвимом положении (возврат активов невозможен), если существует вероятность того, что чрезвычайно опасная информация будет скомпрометирована, или если потенциальное влияние на бизнес намного превышает выплату выкупа, тогда бизнес может решить платить».

Тройная группа вымогателей-вымогателей с агрессивной партнерской программой

Программа-вымогатель Hive имеет одну из самых агрессивных партнерских программ-вымогателей как услуга (RaaS) в мире киберпреступности.

Группа программ-вымогателей «тройного вымогательства» требует от организаций выкуп после шифрования данных, утечки украденных данных и прямого вымогательства у лиц, пострадавших от атак программ-вымогателей.

Хотя его атаки финансово мотивированы, группа вымогателей сотрудничает с политически мотивированными хакерскими группами, такими как программа-вымогатель Conti. Основные цели Hive включают компании в секторах энергетики, здравоохранения, СМИ и образования. Недавние жертвы группировок программ-вымогателей Hive включают службу общественного здравоохранения Коста-Рики и Фонд социального обеспечения (CCSS). Группа вымогателей также взяла на себя ответственность за атаку на New York Racing Association (NYRA), поставщика услуг экстренной помощи Empress EMS и канадскую дочернюю компанию Bell, Bell Technical Solutions. Точно так же программа-вымогатель Hive была ответственна за кибератаку в 2021 году на крупнейшего в Европе продавца бытовой электроники Media Markt.

По данным компании Group-IB, специализирующейся на анализе угроз, к 16 октября 2021 года операторы программ-вымогателей Hive атаковали 355 компаний, что на 72% больше, чем в сентябре 2021 года, при этом 43 жертвы, вероятно, заплатили выкуп в течение одного месяца.

Точно так же Digital Shadows оценила банду Hive RaaS как третью по распространенности группу программ-вымогателей в третьем квартале 2022 года после групп программ-вымогателей LockBit и Black Basta, но впереди BlackCat, Vice Society и AvosLocker.

Векторы атак Hive включают незащищенные и уязвимые RDP-серверы, украденные учетные данные VPN и фишинговые электронные письма с зараженными вложениями.

В августе 2021 года ФБР опубликовало экстренное предупреждение о программе-вымогателе Hive с подробным описанием индикаторов компрометации (IOC) банды, а также тактики, методов и процедур (TTP).

«Повышение шансов на защиту от программ-вымогателей начинается с наблюдения за входной и задней дверью, — сказал Либих.

Он рекомендовал обучать сотрудников методам фишинга, следить за активами и конечными точками вашей организации, устранять уязвимости, искать угрозы, отслеживать подключения и поддерживать регулярное резервное копирование за пределы площадки.

«Лучший способ защититься от программ-вымогателей — никогда не позволять им внедряться в ваши системы. Следующий лучший способ — иметь пуленепробиваемую, надежную стратегию восстановления, чтобы свести к минимуму время простоя и исключить споры о «выкупе». ***(Alicia Hope. Hive Ransomware Group Leaks Stolen Data After Attacking a Major India Power Company // CPO Magazine (https://www.cpomagazine.com/cyber-security/hive-ransomware-group-leaks-stolen-data-after-attacking-a-major-india-power-company/). 04.11.2022).***

***

«Программа-вымогатель — это тип вредоносного программного обеспечения, которое ограничивает доступ к компьютерным системам и данным, хранящимся на них, до тех пор, пока не будет выплачен выкуп. В недавних кибератаках функции программ-вымогателей расширились и теперь включают в себя кражу данных, распределенные атаки типа «отказ в обслуживании» (DDoS) и методы антианализа.

Кроме того, злоумышленники, стоящие за этими атаками, широко применяют модель «программы-вымогатели как услуга» (RaaS). Программа-вымогатель как услуга — это бизнес-модель, которая помогает разработчикам и операторам программ-вымогателей продавать или сдавать в аренду возможности программ-вымогателей злоумышленникам.

Распространенное поведение программ-вымогателей

Основываясь на шаблоне атаки, программы-вымогатели могут шифровать важные данные, не мешая другим функциям компьютерной системы. Этот тип вредоносных программ может запретить доступ ко всему веб-приложению или определенным файлам в компьютерной системе. Это может помешать компаниям просматривать или использовать свои данные или выполнять операционные функции. Примеры включают программы-вымогатели Lockbit 3.0, Black Basta и Pandora.

Типичным поведением некоторых программ-вымогателей является их способность блокировать жертвам доступ к основным функциям устройства. Жертвам программ-вымогателей обычно запрещается дальнейшее взаимодействие со своей операционной системой, оставляя им доступ только для облегчения выплаты выкупа. Примеры включают программы-вымогатели Petya, GoldenEye и KeRanger.

Программы-вымогатели используют тактику двойного вымогательства: шифруют файлы и извлекают данные с намерением опубликовать их, если выкуп не будет выплачен.

После успешных атак программ-вымогателей злоумышленники обычно оставляют сообщения с требованием выкупа в криптовалютах, таких как Биткойн и Монеро. Это гарантирует сохранение анонимности злоумышленника.

Вектор атаки программ-вымогателей

Программы-вымогатели распространяются с использованием различных методов, но наиболее распространенным способом заражения компьютерных систем являются действия, инициированные пользователем. К таким действиям относятся переход по вредоносной ссылке в фишинговых письмах или посещение взломанного веб-сайта. Злоумышленники также используют неверные конфигурации системы, такие как незащищенные подключения к удаленному рабочему столу, доступные через Интернет, и слабые пароли/управление доступом для запуска атак программ-вымогателей.

Существуют и другие формы заражения, использующие вредоносную рекламу и попутные загрузки. Эти формы заражения распространяются без необходимости взаимодействия пользователя с вредоносным ПО.

Влияние атак программ-вымогателей на организации

Атаки программ-вымогателей могут оказать существенное влияние на организации и их способность выполнять важные задачи различными способами. Некоторые способы, которыми это может повлиять на организации, выделены ниже:

Раскрытие конфиденциальных данных. Большинство операторов программ-вымогателей используют методы эксфильтрации данных, чтобы заставить организации платить выкуп после проведения успешной атаки. Обычно они угрожают раскрыть украденные данные в даркнете, если выкуп не будет выплачен.

Увеличенное среднее время восстановления. Атаки программ-вымогателей обычно приводят к тому, что организации теряют доступ к критически важным системам и приложениям на длительный период. Большинство компаний испытывают простои, которые длятся несколько дней, что представляет собой значительный сбой в работе и производительности.

Ущерб репутации бренда. Репутация и ценность бренда большинства организаций несут ущерб из-за атак, связанных с кибербезопасностью, включая программы-вымогатели.

Финансовые потери. Выкуп, выплачиваемый организациями, подвергшимися крупным атакам программ-вымогателей, обычно является дорогостоящим. Эти организации также могут нести дополнительное финансовое бремя со стороны регулирующих органов после инцидента, связанного с безопасностью.

Как Wazuh защищает конечные точки от атак программ-вымогателей

Wazuh — это решение для обеспечения безопасности, которое предлагает унифицированную защиту SIEM и XDR на нескольких платформах. В статье Wazuh — бесплатная платформа XDR с открытым исходным кодом рассказывается, как организации могут воспользоваться преимуществом открытого характера Wazuh, чтобы свободно использовать и настраивать его в соответствии со своими потребностями в области безопасности. Он защищает рабочие нагрузки в виртуализированных, локальных, облачных и контейнерных средах.

Wazuh предлагает несколько возможностей, которые организации могут использовать для обнаружения угроз безопасности и защиты от них. В этом разделе

рассказывается о нескольких возможностях Wazuh, обеспечивающих защиту от атак программ-вымогателей.

Обнаружение уязвимостей

Обнаружение уязвимостей — это процесс выявления слабых мест в операционной системе и программном обеспечении, установленном на конечной точке. В недавно опубликованном Wazuh сообщении в блоге « Обнаружение программы-вымогателя Lockbit 3.0 » отмечается, что одним из векторов атаки программы-вымогателя является использование неисправленных уязвимостей сервера.

Модуль Wazuh Vulnerability Detector выполняет аудит программного обеспечения для обнаружения уязвимостей в конечных точках. Wazuh создает глобальную базу данных уязвимостей из общедоступных репозиториев CVE. Затем Wazuh сопоставляет данные инвентаризации приложений, собранные с конечных точек, с базой данных уязвимостей, чтобы обнаружить уязвимые компоненты.

Оценка конфигурации безопасности (SCA)

Оценка конфигурации безопасности — это процесс, используемый для выявления неправильных конфигураций системы, которые могут подвергать систему атакам. Это включает в себя периодические проверки конфигурации и внедрение передовых методов безопасности путем принятия таких стандартов, как CIS (Центр интернет-безопасности).

Модуль Wazuh Security Configuration Assessment предлагает возможность регулярного сканирования конечных точек, чтобы убедиться, что они соответствуют передовым практикам безопасности. Эти сканирования оценивают конфигурацию конечных точек с помощью файлов политик, содержащих правила, которые необходимо протестировать в сравнении с фактической конфигурацией хоста.

Например, модуль Wazuh SCA проверяет конфигурации, связанные с использованием пароля и нежелательными приложениями и службами. Он также проверяет конфигурацию стека TCP/IP на отслеживаемой конечной точке. В нашей недавней публикации в блоге «Как выполнить оценку безопасности WordPress с помощью Wazuh» показано, как внедрить модуль Wazuh SCA для сравнительного анализа конфигураций WordPress.

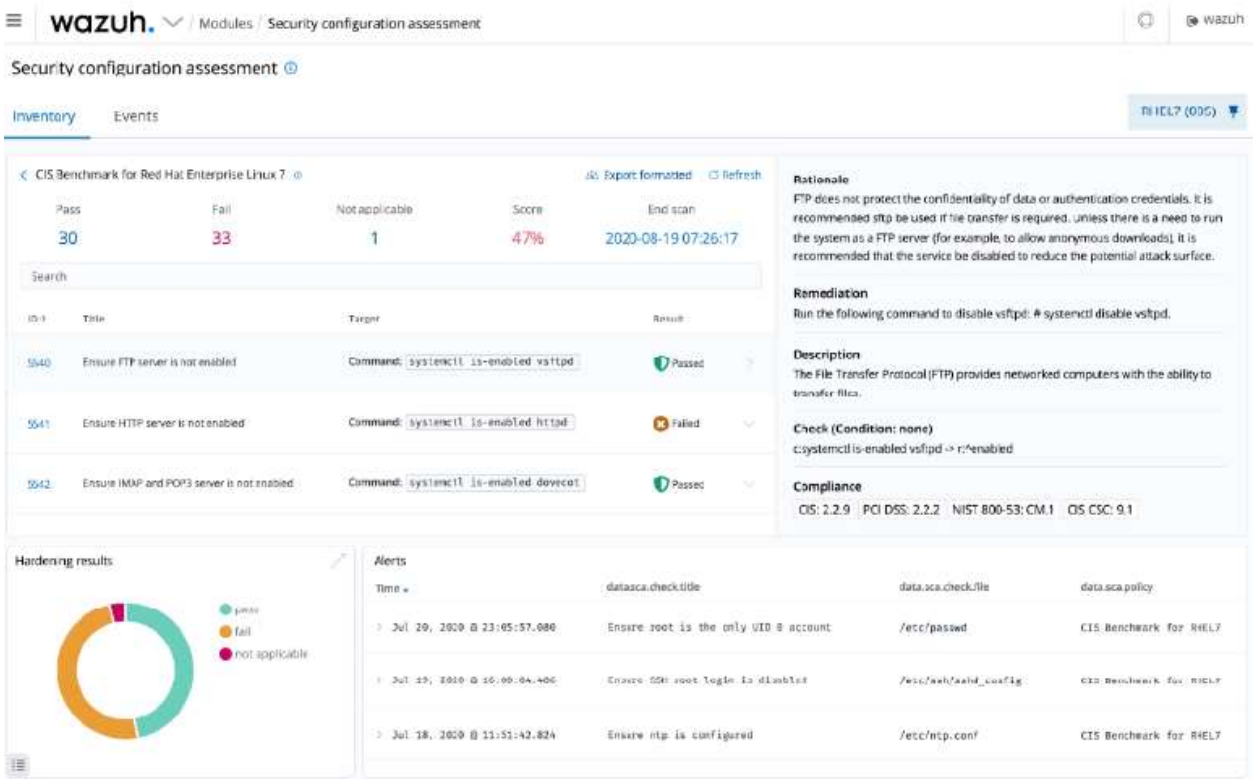


Рис. 1. Панель мониторинга Wazuh, показывающая результат проверки SCA на устройстве Red Hat Enterprise Linux.

Мониторинг целостности файлов

Мониторинг целостности файлов (FIM) — это процесс мониторинга файловой системы конечной точки на предмет действий по добавлению, удалению и изменению. Важно отслеживать важные файлы и каталоги на конечной точке, чтобы гарантировать, что сделанные изменения являются законными.

Модуль Wazuh FIM обнаруживает изменения в отслеживаемых файлах и каталогах, а затем генерирует предупреждение на панели управления Wazuh. Изменения обнаруживаются при наличии расхождений в сохраненной криптографической контрольной сумме и других атрибутах отслеживаемых файлов и каталогов на конечной точке. Мониторинг файлов и каталогов осуществляется периодически или почти в режиме реального времени.

Как показано в этом сообщении в блоге, модуль Wazuh FIM можно использовать для обнаружения наличия программ-вымогателей на конечной точке. Большинство атак программ-вымогателей инициируют выполнение путем переноса вредоносных файлов в определенные каталоги, и модуль Wazuh FIM может обнаружить такую активность.

Wazuh можно интегрировать с другими решениями для обеспечения безопасности, такими как VirusTotal и YARA, для сканирования файлов на конечных точках и проверки того, являются ли они безвредными или вредоносными. Модуль активного реагирования Wazuh удаляет обнаруженные файлы программ-вымогателей.

На рисунке 2 ниже показан пример интеграции Wazuh с YARA для обнаружения программы-вымогателя Lockbit 3.0. Модуль активного реагирования удалил файл программы-вымогателя после его обнаружения.

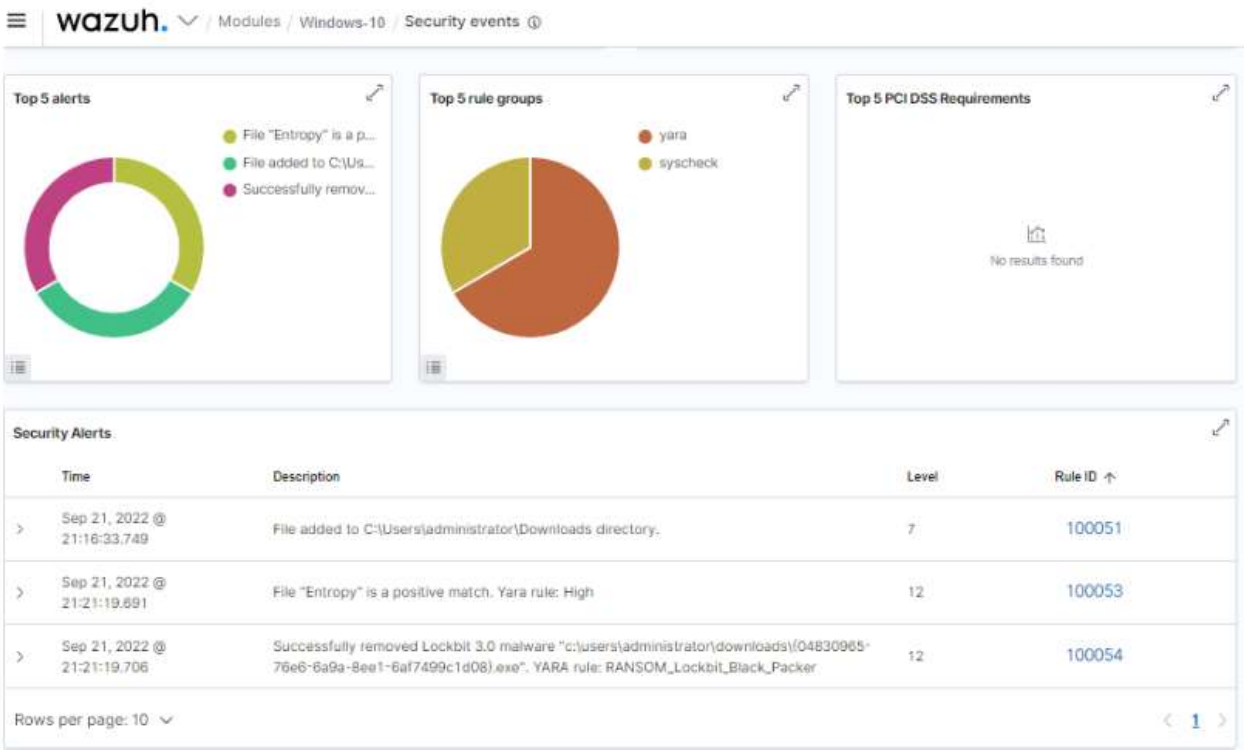


Рисунок 2. Интеграция Wazuh с YARA для обнаружения исполняемого файла программы-вымогателя

Обнаружение с помощью Wazuh

На начальном этапе атаки программ-вымогателей вредоносное ПО выполняет несколько действий на зараженной конечной точке.

Эти действия могут включать удаление службы теневого тома, отключение службы защиты от вредоносных программ, очистку журналов средства просмотра событий Windows, создание заметок о программах-вымогателях в нескольких каталогах и изменение фона рабочего стола.

Это поведение может быть зафиксировано с помощью готовых правил и декодеров Wazuh и оповещено на панели управления Wazuh практически в режиме реального времени. Пользовательские правила обнаружения также можно настроить и сопоставить с соответствующими тактиками и методами MITRE ATT&CK для обнаружения таких событий.

Вывод

Из-за постоянно меняющейся динамики атак программ-вымогателей организациям необходимо применять адекватные меры безопасности. Концепция RaaS упростила и сделала злоумышленникам более выгодным нацеливание на организации программ-вымогателей. Организации могут эффективно обнаруживать атаки программ-вымогателей, используя различные возможности Wazuh, как обсуждалось выше.

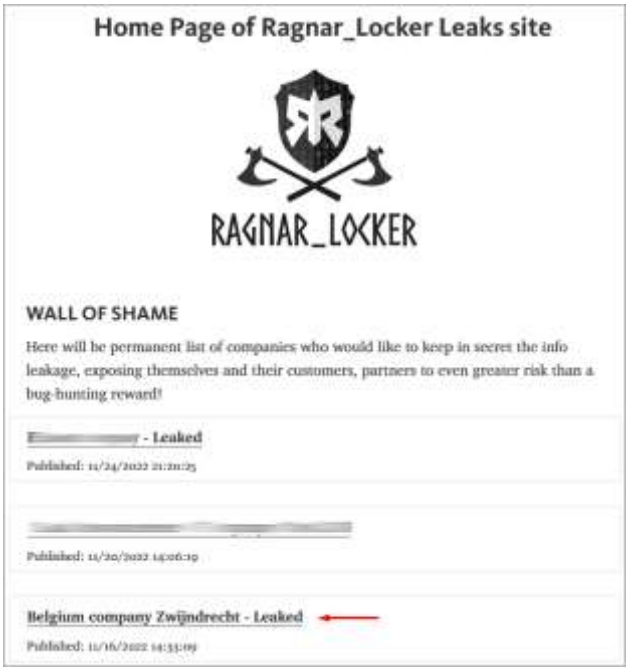
Wazuh — это бесплатное решение SIEM и XDR с открытым исходным кодом, которое ежегодно загружают более 10 миллионов раз и постоянно растущим сообществом. Wazuh хорошо интегрируется с несколькими сторонними решениями и технологиями…» ***(Wazuh. Ransomware detection with Wazuh SIEM and XDR platform // Bleeping Computer®***

(https://www.bleepingcomputer.com/news/security/ransomware-detection-with-wazuh-siem-and-xdr-platform/). 29.11.2022).

***

«Банда вымогателей Ragnar Locker опубликовала украденные данные из того, что они считали муниципалитетом Звейндрехт, но оказалось, что они были украдены из полиции Звейндрехта, местного полицейского подразделения в Антверпене, Бельгия.

Сообщается, что просочившиеся данные выявили тысячи автомобильных номеров, штрафы, файлы отчетов о преступлениях, данные о персонале, отчеты о расследованиях и многое другое.



Рагнар Локер указал не ту жертву (BleepingComputer)

Этот тип данных может потенциально разоблачить людей, сообщивших о преступлениях или злоупотреблениях, и поставить под угрозу текущие операции и расследования правоохранительных органов.

Бельгийские СМИ называют эту утечку данных одной из крупнейших в своем роде, которая затронула государственную службу в стране, раскрывая все данные, хранившиеся полицией Звейндрехта с 2006 по сентябрь 2022 года.

Полиция подтверждает нападение

Полиция Звейндрехта отреагировала на освещение в местных СМИ сообщением в Facebook, преуменьшив влияние инцидента и заявив, что хакеры получили доступ только к той части сети, где полиция хранила административные данные.

В полиции говорят, что злоумышленники могли получить доступ к данным только в административной сети, поэтому в первую очередь пострадал персонал.

Заявление полиции Звейндрехта на Facebook

Начальник полиции Звиндрехта Марк Снелс сообщил новостной сети VRT, что утечка данных произошла из-за человеческой ошибки, и теперь они связываются со всеми пострадавшими, чтобы сообщить им об инциденте.

«Это не тот случай, когда произошла утечка всех данных. Эта сеть в основном содержит личную информацию от наших сотрудников, такую как списки персонала и фотографии с партий персонала», — прокомментировал Снелс местным СМИ.

«Но это правда, что иногда в этой сети есть конфиденциальная информация, хотя мы всегда стараемся размещать ее только в профессиональной сети. Это человеческие ошибки. Например, просочились также штрафы и PV. насилие. Это, конечно, очень больно». - Начальник полиции Звейндрехта.

Более широкое воздействие, чем заявлено

Хотя этот инцидент не затронул сеть национальной полиции Бельгии, брешь в местной сети Zwijndrecht по-прежнему имеет большое значение для тысяч людей.

Бельгийский журналист Кеннет Ди опубликовал новость об атаке на Het Laatste Nieuws, поделившись тем, что злоумышленники якобы атаковали плохо защищенную конечную точку Citrix, чтобы взломать полицейскую сеть.

Расследование данных, проведенное Ди, выявило метаданные абонентов телекоммуникационных услуг и SMS людей, находящихся под тайным полицейским расследованием.

Кроме того, просочившиеся файлы содержат кадры с дорожных камер, раскрывающие местонахождение людей в определенные даты и время.

«Это крупнейшая утечка информации из правоохранительных органов в истории Бельгии и, возможно, самая серьезная утечка, которую мы когда-либо видели в нашей стране», — сказал Ди Bleeping Computer.

«Это должно быть тревожным звонком для местной полиции и того, как они обрабатывают данные граждан, и, надеюсь, это приведет к изменениям на этом фронте».

Управление по защите данных страны еще не объявило о расследовании дела, но прокуратура возбудила уголовное дело, которое сосредоточено на самом инциденте со взломом.

Бельгийский юрист и активист по защите конфиденциальности Матиас Доббелар-Велварт сказал BleepingComputer, что незащищенные лица должны менять все, что могут, включая номерные знаки, удостоверения личности, паспорта и т. д.

«Вы не можете легко сменить место жительства, но даже если вы измените все документы, последствия этого инцидента с безопасностью могут быть на всю жизнь, а кража личных данных — это не шутки», — говорит Доббелар-Велварт.

«Я считаю, что пока не все полицейские сетевые системы защищены должным образом, ни одна смарт-камера не должна включаться». ***(Bill Toulas. Ransomware gang targets Belgian municipality, hits police instead // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ransomware-gang-targets-belgian-municipality-hits-police-instead/). 26.11.2022).***

***

«Новые атаки программ-вымогателей, нацеленные на организации в Украине, впервые обнаруженные в этот понедельник, были связаны с печально известной российской военной группировкой Sandworm.

Словацкая компания-разработчик программного обеспечения ESET, которая первой заметила эту волну атак, говорит, что программа-вымогатель, которую они назвали RansomBoggs, была обнаружена в сетях нескольких украинских организаций.

«Хотя вредоносное ПО, написанное на.NET, является новым, его развертывание аналогично предыдущим атакам, приписываемым Sandworm», — заявили в исследовательской лаборатории ESET.

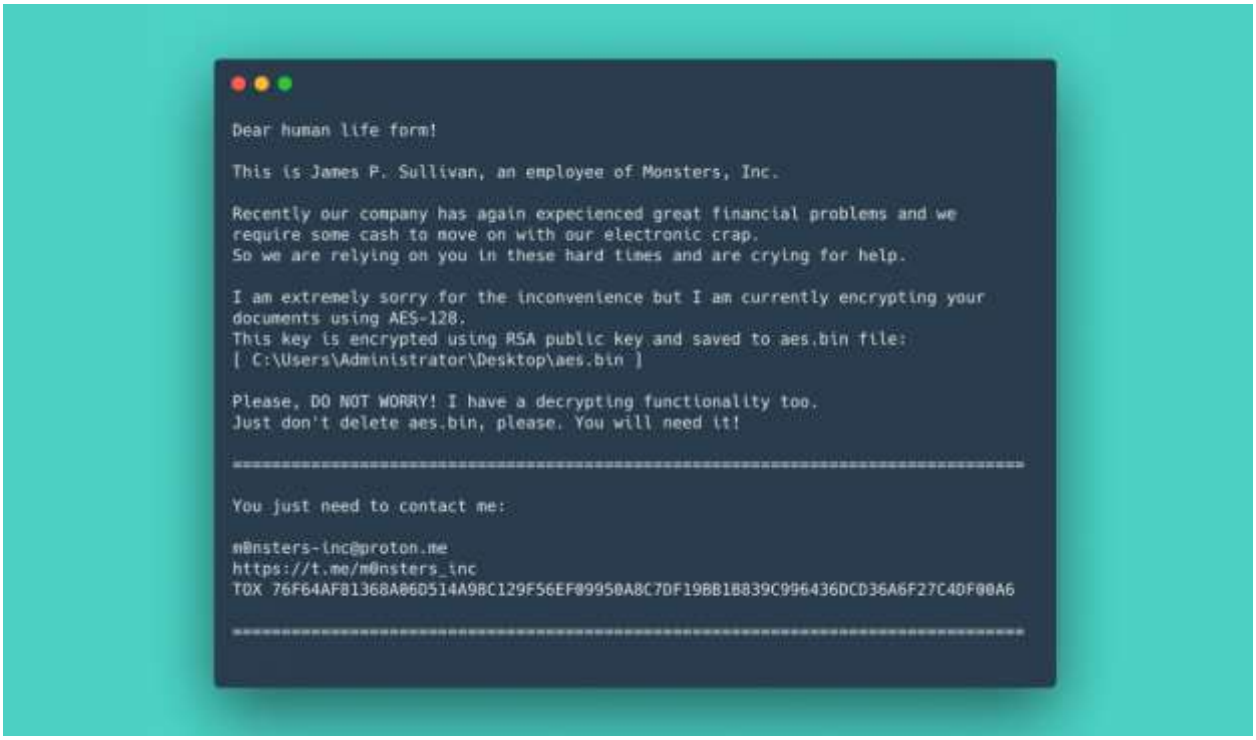
«Есть сходство с предыдущими атаками, проведенными Sandworm: сценарий PowerShell, используемый для распространения программы-вымогателя.NET с контроллера домена, почти идентичен тому, который был замечен в апреле прошлого года во время атак Industroyer2 против энергетического сектора».

Сценарий PowerShell, используемый для развертывания полезной нагрузки RansomBoggs в сетях жертв, известен как POWERGAP и также стоял за доставкой деструктивного вредоносного ПО CaddyWiper при атаках на украинские организации в марте.

После передачи по сети жертвы RansomBoggs шифрует файлы, используя AES-256 в режиме CBC, используя случайный ключ (сгенерированный случайным образом, зашифрованный RSA и записанный в aes.bin), и добавляет расширение.chsch ко всем расширениям зашифрованных файлов.

В зависимости от варианта атаки открытый ключ RSA может быть жестко запрограммирован в самой вредоносной программе или предоставлен в качестве аргумента.

В зашифрованных системах программа-вымогатель также сбрасывает заметки с требованием выкупа, выдавая себя за Джеймса П. Салливана, главного героя фильма «Корпорация монстров», с дополнительными ссылками, которые также можно найти в коде вредоносной программы.



Записка о выкупе RansomBoggs (ESET)

Ранее в этом месяце Microsoft также связала группу кибершпионажа Sandworm (отслеживаемую Redmond как IRIDIUM) с атаками программ-вымогателей Prestige, нацеленных на транспортные и логистические компании в Украине и Польше с октября.

«Кампания «Престиж» может подчеркнуть взвешенный сдвиг в расчете разрушительных атак IRIDIUM, сигнализируя о повышенном риске для организаций, напрямую поставляющих или транспортирующих гуманитарную или военную помощь Украине», — говорится в сообщении MSTIC.

«В более широком смысле это может представлять повышенный риск для организаций в Восточной Европе, которые могут рассматриваться российским государством как оказывающие поддержку в связи с войной».

В феврале совместные рекомендации по безопасности, выпущенные агентствами кибербезопасности США и Великобритании, также привязали ботнет Cyclops Blink к российской военной группе угроз до ее разрушения, что предотвратило его использование в дикой природе.

Sandworm — группа элитных российских хакеров, действовавшая не менее двух десятилетий и предположительно входящая в состав подразделения 74455 Главного центра специальных технологий (ГЦСТ) ГРУ России.

Ранее они были связаны с атаками, приведшими к атакам KillDisk Wiper, нацеленным на банки в Украине, и украинским отключениям электроэнергии в 2015 и 2016 годах.

Также считается, что Sandworm разработал программу-вымогатель NotPetya, которая нанесла миллиардный ущерб начиная с июня 2017 года…». ***(Sergiu Gatlan. New ransomware attacks in Ukraine linked to Russian Sandworm hackers // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-ransomware-attacks-in-ukraine-linked-to-russian-sandworm-hackers/).*** 25.11.2022).

***

«…Угроза программ-вымогателей быстро растет, а последствия атаки огромны. Вопрос не в том, «если», а в том, «когда» вы столкнетесь с этой проблемой. Выбор между выплатой выкупа или потерей данных является дорогостоящим и рискованным.

Расходы, связанные с кибератаками, в том числе потеря бизнеса, повышение страховых ставок, судебные иски, уголовные расследования и плохая пресса, могут даже вывести компанию из бизнеса — и быстро! Вот лишь некоторые из множества утечек данных, произошедших за последние 18 месяцев, и их дорогостоящие потери:

• The New York Times сообщила, что T-Mobile достигла урегулирования в размере 500 миллионов долларов после масштабной утечки данных в 2021 году. Компания, которая заявила, что атака затронула 76,6 миллиона человек, согласилась выплатить 350 миллионов долларов для урегулирования претензий и потратить 150 миллионов долларов на укрепление безопасности.

• Insider сообщил, что глобальная страховая компания CNA Financial раскошелилась на 40 миллионов долларов после кибератаки в прошлом году.

• The Washington Post сообщила, что атака программы-вымогателя на американского поставщика программного обеспечения Kaseya в 2021 году, нацеленная на инструмент удаленного управления компьютерами фирмы, поставила под угрозу до 2000 компаний по всему миру.

Существует множество стратегий подготовки и снижения рисков, связанных с угрозами кибербезопасности, такими как программы-вымогатели, но каждая из них сопряжена со своим набором проблем. Резервное копирование является важнейшим средством восстановления, и все же корпоративные решения для резервного копирования, которым уже несколько десятков лет, не рассчитаны на работу с масштабом и сложностью современных данных. И эта проблема продолжает расти. Как ранее в этом году отмечало SearchDataManagement, к 2025 году ожидается, что объем коллективных данных в мире достигнет 175 зеттабайт (число 175 с 21 нулем).

Резервная копия не работает

Традиционное резервное копирование, как мы знаем, не работает. Вот почему:

• Резервные копии периодически создаются пакетами. Когда требуется восстановление данных, последняя доступная копия может быть старше 24 часов, что приводит к безвозвратной потере данных и/или недавних изменений.

• Резервное копирование устарело — устаревшее программное обеспечение для резервного копирования на основе снэпшотов, разработанное несколько десятилетий назад, по-прежнему использует агенты для защиты и восстановления виртуальных машин, что приводит к высоким затратам на обслуживание, потере времени на администрирование или даже неудачному восстановлению.

• Это дорого — помимо затрат, связанных с влиянием на производительность и ресурсы, устаревшее резервное копирование требует нескольких лицензий, дополнительных покупок агентов и увеличения затрат на ИТ-инфраструктуру.

• Устаревшие инструменты резервного копирования сложны — они используют распределенные системы для передачи данных, требующие специального оборудования, обширной конфигурации и большого количества времени и ресурсов ИТ.

• Это разрушительно — устаревшие задания резервного копирования часто не выполняются вовремя, нарушая работу производственной среды из-за незапланированных простоев и сильно нагружая и без того ограниченные ИТ-ресурсы.

• И это медленно. Устаревшие процессы резервного копирования создают огромную нагрузку на производственную среду, вызывая задержку сети и время простоя.

Новая парадигма резервного копирования для почти мгновенного восстановления данных

Что необходимо, так это непрерывное резервное копирование в режиме реального времени. Эта возможность обеспечит надежную первую линию защиты от угроз кибербезопасности, позволяя организациям легко и почти мгновенно восстанавливать скомпрометированные данные.

Традиционно резервное копирование находится вне пути к данным операционной системы. Поскольку данные продолжают расти в геометрической прогрессии — как по количеству файлов, так и по количеству генерируемых данных — системы резервного копирования, которые сканируют файловые системы, больше невозможны, особенно когда мы вступаем в мир миллиардов файлов и петабайтов или более данных.

Новый подход будет переплетать резервное копирование с самой системой данных, а не существовать вне ее, позволяя немедленно записывать все сканирования и сохранения файлов без риска потери при обмене данными между двумя системами. Кроме того, сохранение и сканирование будут происходить постоянно — не только тогда, когда пользователь вносит изменения в файл, но и в любой момент на протяжении всего его жизненного цикла.

Эта модель объединит файловую систему и резервное копирование в один объект, что позволит организациям легко и молниеносно восстанавливать скомпрометированные данные, предоставляя им доступ ко всем данным в том виде, в каком они существовали непосредственно перед злоумышленной атакой или компрометацией системы. Это позволит организациям быстро восстанавливать свои данные и избежать огромных затрат времени и средств, связанных с потерей или повреждением данных.

Текущие решения для резервного копирования и восстановления не соответствуют требованиям мира, но это не значит, что мы должны соглашаться на меньшее. В 2023 году повышенное внимание будет уделяться «первой линии защиты», где кибератаки полностью останавливаются или могут быть быстро развернуты без обращения к резервным копиям. Вместо того, чтобы занимать часы, дни, а иногда и недели и более, выздоровление наступало почти мгновенно.

Подход на основе метаданных, который находится внутри пути к данным операционной системы, может обеспечить непрерывный доступ к данным. Этот метод может обеспечить беспрецедентную защиту данных, позволяя приблизиться к идеальному нулевому целевому времени восстановления (RTO), предоставляя пользователям контроль над поиском и восстановлением данных немедленно без помощи ИТ-специалистов, и нулевую целевую точку восстановления (RPO), устраняя значительные затраты и последствия прерывания доступа к данным.

Все, что больше, является компромиссом, который подвергает организации повышенному риску потери данных и финансовых потерь. Компании должны подталкивать поставщиков к достижению RPO и RTO, равных нулю или как можно ближе к нулю, и искать решения, которые достигают этих целей». ***(Jason Lohrey. Cybersecurity Threats Need Fresh Data Recovery Strategies// Techstrong Group Inc. (https://securityboulevard.com/2022/11/cybersecurity-threats-need-fresh-data-recovery-strategies/). 28.11.2022).***

***

«Раніше невідома програма-вимагач ARCrypter, яка скомпрометувала чимало організацій в Латинській Америці, розширює свої атаки по всьому світу.

За словами експертів The BlackBerry Research and Intelligence Team, ARCrypter зараз розширює свою діяльність за межами Латинської Америки і націлений на різні організації по всьому світу, у тому числі в Китаї, Канаді, Німеччині, США та Франції.

Вимоги викупу в кожному випадку варіюються та сягають $ 5000. Експерти пояснюють це тим, що ARCrypter є програмою-вимагачем середнього рівня. У дослідженні були опубліковані деталі того, як вірус зламує пристрій користувача та шифрує більшу частину даних з метою вимагання.

BlackBerry зазначили, що перші зразки ARCrypter з'явилися на початку серпня 2022 року за кілька тижнів до першої серйозної атаки в Чилі. В даний час про розробників ARCrypter майже нічого не відомо — їхнє походження, мова та потенційні зв'язки з іншими угрупованнями». ***(Вірус-вимагач ARCrypter поширюється по всьому світу // Internetua (https://internetua.com/virus-vimagacs-arcrypter-poshiruayetsya-po-vsomu-svitu). 20.11.2022).***

***

«Компания OpenText™ (NASDAQ: OTEX) (TSX: OTEX) сегодня опубликовала результаты глобального исследования программ-вымогателей OpenText Security Solutions 2022 для малого и среднего бизнеса (SMB). Результаты показывают растущую озабоченность по поводу атак программ-вымогателей, влияния геополитической напряженности и роста инфляции. Восемьдесят восемь процентов респондентов отметили, что они обеспокоены или крайне обеспокоены атакой, которая повлияет на их бизнес.

«Малый и средний бизнес — это выгодное место для хакеров, потому что им часто не хватает ресурсов кибербезопасности, как технологий, так и опыта в области безопасности», — сказал Прентисс Донохью, исполнительный вице-президент OpenText Security Solutions. «Сегодняшняя сложная картина угроз представляет огромный риск для малых и средних предприятий, которые не имеют достаточной подготовки к киберустойчивости, чтобы остановить распространение и быстро восстановиться после атаки. Поскольку злоумышленники становятся все более изощренными и безжалостными, многоуровневая стратегия защиты больше не является хорошей. иметь, это необходимость».

Основные выводы:

Малые и средние предприятия опасаются сокращения бюджетов на безопасность на фоне растущей обеспокоенности ростом рисков программ-вымогателей из-за обострения геополитической напряженности.

Более половины (57%) малых и средних предприятий обеспокоены сокращением своего бюджета на кибербезопасность на фоне роста инфляции.

52% респондентов считают, что риск атаки программ-вымогателей выше из-за обострения геополитической напряженности.

84% обеспокоены атакой программы-вымогателя, которая повлияет на их бизнес.

Существует тревожная неосведомленность среди малого и среднего бизнеса, когда дело доходит до того, чтобы узнать, подверглись ли они атаке программ-вымогателей. При этом бюджеты на защиту от этих рисков невелики.

Почти половина (46%) предприятий малого и среднего бизнеса подверглись атаке программ-вымогателей, но 67% до сих пор не думают или не уверены, что они являются целью программ-вымогателей.

Большинство (60%) респондентов не уверены или лишь частично уверены в том, что смогут отразить атаку программ-вымогателей.

Несмотря на то, что многие уже сталкивались с атаками ранее, бюджеты безопасности минимальны для защиты от программ-вымогателей и других угроз:

60% тратят менее 50 000 долларов в год.

50% тратят менее 20 000 долларов в год.

Только 10% тратят более 50 000 долларов в год.

Поставщики управляемых услуг (MSP) являются привлекательным вариантом безопасности для малого и среднего бизнеса, позволяющим компенсировать ограничения ресурсов.

Больше малых и средних предприятий передают свою безопасность на аутсорсинг ИТ-провайдеру или MSP, при этом 58% используют внешнюю поддержку управления безопасностью.

В то же время 65% предприятий малого и среднего бизнеса, которые в настоящее время не используют MSP, рассмотрят возможность использования этого в будущем…

В период с 24 сентября по 10 октября 2022 года компания OpenText Security Solutions опросила 1332 специалиста по безопасности и ИТ-специалистов из малого и среднего бизнеса (SMB), до 1000 сотрудников в США, Великобритании и Австралии. Респонденты представляли ряд ролей, от сотрудников службы безопасности и технических специалистов до руководителей высшего звена, а также в различных отраслях, включая технологии, розничную торговлю, образование, производство, здравоохранение и многое другое…» ***(OpenText Security Solutions Global SMB Ransomware Survey Reveals Heightened Worry about Increased Cyber Attacks Due to Geopolitical Tensions // Cision US Inc. (https://www.prnewswire.com/news-releases/opentext-security-solutions-global-smb-ransomware-survey-reveals-heightened-worry-about-increased-cyber-attacks-due-to-geopolitical-tensions-301670320.html). 07.11.2022).***

***

«Фишинговая кампания, нацеленная на сотрудников Dropbox, привела к компрометации 130 репозиториев компании на GitHub, поскольку злоумышленник засыпал сотрудников электронными письмами, ведущими на поддельные страницы входа, и в конечном итоге сумел взломать одну из них. Нарушение безопасности не представляет непосредственной угрозы для учетных записей пользователей Dropbox, но, как сообщается, предоставило злоумышленникам инструменты разработчика, включая ключи API.

Нарушение безопасности Dropbox приводит к утечке кода и инструментов разработчика

Dropbox заявляет, что нарушение безопасности не касалось содержимого каких-либо учетных записей клиентов, а также какой-либо контактной или платежной информации. Тем не менее, он включал некоторые имена и адреса электронной почты сотрудников компании и деловых контактов.

Вместо этого злоумышленники сосредоточились на репозиториях GitHub компании, взломав 130 из них в поисках кода и инструментов. Dropbox говорит, что это включало внутренние учетные данные, в качестве примера называя ключи API разработчика.

Нарушение безопасности, похоже, началось 13 октября; подозрительная активность была отмечена в репозиториях GitHub компании, а 14 октября Dropbox был уведомлен, что привело к обнаружению того, что сотрудник был скомпрометирован фишинговым электронным письмом.

Злоумышленники разослали фишинговые электронные письма ряду сотрудников Dropbox, выдавая себя за широко используемую интеграционную платформу CircleCI DevOps (которая позволяет использовать учетные данные GitHub в качестве логина). Злоумышленник перехватил их регистрационную информацию и предложил сотрудникам использовать свой аппаратный ключ аутентификации для отправки одноразового пароля на сайт атаки, открывая им дверь для рейдов в репозитории GitHub.

Объем личной информации, потерянной в результате этого нарушения безопасности, относительно минимален; «несколько тысяч» имен и адресов электронной почты, принадлежащих нынешним и бывшим сотрудникам Dropbox, руководителям отдела продаж, поставщикам и клиентам (из примерно 700 миллионов пользователей платформы). Dropbox заявляет, что клиентам не о чем беспокоиться с точки зрения содержимого их хранилища или их платежной информации, и что они привлекли внешних экспертов-криминалистов для проверки масштабов нарушения безопасности.

Хотя клиенты не подвергаются непосредственному риску, нарушение безопасности, связанное с внутренними материалами разработчиков, всегда вызывает постоянную озабоченность. Неясно, что именно было взято из репозиториев GitHub помимо некоторых ключей API, но это те материалы, которые можно проанализировать для поиска уязвимостей, которые можно использовать, а также могут предоставить другие типы ключей или токенов, которые позволят злоумышленникам расширить свой диапазон. доступа.

Доктор Эрик Коул, член консультативного совета Theon Technology, считает, что еще больше плохих новостей еще впереди, поскольку полное влияние на репозитории GitHub намечено: «Если это будет похоже на другие нарушения в течение следующих нескольких недель, 130 репозиториев увеличатся. до 1300 или 13000. Кроме того, репозиторий может быть очень большим, содержать множество подкаталогов и много файлов, поэтому говорить о 130 репозиториях очень расплывчато, и это может быть большой объем информации. Поскольку репозитории содержат много данных, это также поднимает флаг, когда компания заявляет, что конфиденциальные данные не были скомпрометированы. Лучшим ответом было бы то, что конфиденциальные данные не должны находиться в этих репозиториях, но любой, кто работал с Dropbox или GitHub, знает, что данные часто копируются или хранятся в каталогах, в которых они не должны храниться.

Фишинг расширяется, охватывая вторичные методы аутентификации по мере расширения использования MFA.

Dropbox выпустила заявление, в котором указывалось, что она принимает более устойчивые к фишингу формы MFA для своих сотрудников, начиная с WebAuthn (который также является вариантом, предлагаемым клиентам Dropbox). Система FIDO, которая лежит в основе WebAuthn, предлагает некоторые функции защиты от фишинга, которых нет в других системах, такие как расширенная проверка подлинности подключаемого сайта на основе браузера и пары ключей, которые имеют более конкретное и ограниченное использование.

Так же, как многие компании только начинают осознавать потребность в MFA в своих сетях, те, которые уже внедрили его, обнаруживают, что им нужны еще более безопасные системы, чтобы идти в ногу с современными атаками. Нарушение репозиториев GitHub демонстрирует, что хорошо продуманной фишинговой атаки по электронной почте по-прежнему достаточно, чтобы обойти некоторые меры MFA, даже методы с локальным ключом аутентификации, которые рекламируются как более безопасные. Но злоумышленники добавляют еще более сложные уровни к схемам фишинга, чтобы учесть более широкое использование 2FA и MFA, с возрождением использования SMS-фишинга и телефонных звонков с использованием социальной инженерии в качестве компонентов нарушения безопасности.

Мика Аалто, соучредитель и генеральный директор Hoxhunt, описывает один из этих недавних подходов: «С точки зрения автоматизации хакеры используют ботов, таких как SMSRanger и BloodOTPbot, которые автоматически последуют за атакой по сбору учетных данных с помощью телефонного звонка с использованием тщательно продуманный сценарий социальной инженерии, который заканчивается получением кода аутентификации жертвы. Эти боты станут только умнее и опаснее с развитием таких технологий, как искусственный интеллект».

Пока нет какой-либо известной связи с недавней кампанией, нацеленной на компании, использующие услуги управления доступом Okta, но есть много общего. Злоумышленники Окта разослал SMS-сообщения сотрудникам компаний, о которых известно, что они подписаны на услугу, со ссылками на фишинговую страницу, которая в конечном итоге перехватила учетные данные около 130 организаций. Cloudflare подверглась серьезной атаке во время этой кампании, но объяснила свою

способность предотвращать нарушения безопасности своей более совершенной системой проверки аппаратного ключа. В отчете компании об инциденте говорится, что трое ее сотрудников действительно перешли по фишинговым ссылкам и ввели учетные данные, но функция «привязки источника» их аппаратных ключей FIDO2 в конечном итоге остановила проверку. Компания также выразила уверенность, что ее система мер безопасности конечных точек предотвратит развитие атаки, даже если учетная запись сотрудника будет скомпрометирована.

Ник Раго, полевой технический директор Salt Security, рассматривает взлом репозиториев GitHub как еще один призыв к организациям внедрить архитектуру с нулевым доверием: «Поскольку методы атак с использованием социальной инженерии становятся все более и более изощренными, организации должны максимально использовать менталитет нулевого доверия с артефактами кода, чтобы опережать угрозы. это может возникнуть, когда посторонний человек получает доступ к репозиториям GitHub. В этом случае Dropbox подтвердил, что код, к которому обращался злоумышленник, содержал ключи API, используемые разработчиками Dropbox. Из уведомления об инциденте неясно, для чего использовались эти ключи API, к каким системам они подключались (внутренним или внешним), а также объем данных и функциональный доступ, который субъект угрозы имел бы с этими ключами API. Статические ключи API и другие важные учетные данные, используемые разработчиками приложений, должны быть каким-то образом защищены и не должны храниться в виде простого текста как часть исходного кода приложения, находящегося в состоянии покоя. Шифрование данных или использование безопасного хранилища данных предоставляют две распространенные и более безопасные альтернативы. Нарушение Dropbox служит хорошим напоминанием для организаций о необходимости сканировать свои репозитории исходного кода, чтобы найти любые учетные данные, хранящиеся в виде простого текста (ключи API, пароли и т. д.), которые потенциально может использовать злоумышленник, если они получат доступ к репозиторию. Кроме того, этот тип угроз показывает, почему организациям требуется безопасность API во время выполнения, которая может обнаруживать и предотвращать злоупотребление API, если ключ API был скомпрометирован и использован в атаке API». Шифрование данных или использование безопасного хранилища данных предоставляют две распространенные и более безопасные альтернативы. Нарушение Dropbox служит хорошим напоминанием для организаций о необходимости сканировать свои репозитории исходного кода, чтобы найти любые учетные данные, хранящиеся в виде простого текста (ключи API, пароли и т. д.), которые потенциально может использовать злоумышленник, если они получат доступ к репозиторию. Кроме того, этот тип угроз показывает, почему организациям требуется безопасность API во время выполнения, которая может обнаруживать и предотвращать злоупотребление API, если ключ API был скомпрометирован и использован в атаке API». Шифрование данных или использование безопасного хранилища данных предоставляют две распространенные и более безопасные альтернативы. Нарушение Dropbox служит хорошим напоминанием для организаций о необходимости сканировать свои репозитории исходного кода, чтобы найти любые учетные данные, хранящиеся в виде простого текста (ключи API, пароли и т. д.), которые потенциально может

использовать злоумышленник, если они получат доступ к репозиторию. Кроме того, этот тип угроз показывает, почему организациям требуется безопасность API во время выполнения, которая может обнаруживать и предотвращать злоупотребление API, если ключ API был скомпрометирован и использован в атаке API».

Уильям Глейзер, директор по исследованию угроз в Cequence Security, дополнительно отмечает этот инцидент как напоминание о том, что ключи API необходимо постоянно тщательно отслеживать и контролировать, чтобы предотвратить нарушения безопасности: «Ключи API являются ценной целью для злоумышленников. Этот инцидент демонстрирует, почему так важно поддерживать строгую гигиену ключей API. Это включает в себя никогда не проверять API-ключи в репозиториях системы управления версиями, придерживаться принципов ролей доступа с минимальными привилегиями для ключей API и регулярно их чередовать. Хотя в случае с Dropbox первоначальный взлом произошел с помощью фишинга, важно иметь представление о инвентаризации и схеме вашего API во время выполнения. Также важно, чтобы организации гарантировали, что конфиденциальные данные, такие как ключи API, не будут раскрыты через какие-либо неизвестные или недокументированные конечные точки API, и чтобы организации могли аннулировать открытые ключи и восстановить новые». ***(Scott Ikeda. Dropbox Security Breach Leads to Compromise of 130 GitHub Repositories // CPO Magazine (https://www.cpomagazine.com/cyber-security/dropbox-security-breach-leads-to-compromise-of-130-github-repositories/). 07.11.2022).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Застройщик из Джорджии, который десять лет назад украл около 50 000 биткойнов с киберпреступного сайта Silk Road, в пятницу признал себя виновным в мошенничестве с использованием электронных средств связи. Пират Робертс».

Судебные иски показывают, что 32-летний Джеймс «Джимми» Чжун в 2012 году воспользовался уязвимостью в криптовалютном кошельке Silk Road, вызванной быстрым выводом средств за миллисекунды. Он украл криптовалюту на сумму около 577 000 долларов, основываясь на таблице исторической стоимости биткойнов. Разделив украденные средства в попытке скрыть их происхождение, Чжун хранил биткойны на устройствах, хранящихся в подземном сейфе, а «одноплатный компьютер» хранился в банке для попкорна в туалете под кучей одеял.

По крайней мере, именно там их нашел криминальный агент IRS во время рейда 9 ноября 2021 года в доме Чжуна в Гейнсвилле, штат Джорджия, который также обнаружил более 500 000 долларов наличными, по-видимому, драгоценными металлами и 25 физическими биткойн-токенами, известными как монеты Casascius, на сумму около 174 биткойна. Во время федерального рейда возвращенная

украденная криптовалюта стоила 3,36 миллиарда долларов, что, по словам Министерства юстиции, было на тот момент крупнейшим федеральным изъятием криптовалюты и остается вторым по величине финансовым изъятием за всю историю. Сейчас восстановленная криптовалюта стоит около 1 миллиарда долларов.

Чжун заключил сделку о признании вины, требующую, чтобы он лишился украденных биткойнов, наличных денег и содержимого своего сейфа, а также своей 80% доли в RE&D Investments, компании по недвижимости в Мемфисе, штат Теннесси, которая ведет судебный иск кредиторов в федеральном суде. суд по делам о банкротстве с сентября. Чжуну грозит до 20 лет тюрьмы после того, как он признал себя виновным по одному пункту обвинения в мошенничестве с использованием электронных средств связи.

ФБР арестовало Ульбрихта в 2013 году в публичной библиотеке Сан-Франциско, когда он вошел в торговый центр нелегального рынка Silk Road со своего ноутбука в качестве системного администратора, используя свое вымышленное имя, Ужасный пират Робертс. С момента основания веб-сайта в 2011 году Ульбрихт заплатил около 650 000 долларов в схемах убийства по найму, хотя ни одна из пяти предполагаемых жертв на самом деле не умерла в результате.

После ареста Ульбрихт отклонил предложение о признании вины как минимум на 10 лет. После суда присяжных, в результате которого он был осужден за семь уголовных преступлений, Ульбрихт теперь отбывает двойное пожизненное заключение без возможности условно-досрочного освобождения в тюрьме строгого режима в Тусоне, штат Аризона. В июне федеральный судья отклонил попытку Ульбрихта отменить приговор на конституционных основаниях.

У федеральной прокуратуры есть постоянный приказ о конфискации Ульбрихта, а это означает, что криптовалюта, изъятая у Чжуна, теперь является федеральной собственностью.

Чжун смог украсть биткойн после того, как обнаружил, что он может заставить систему обработки платежей Silk Road выплатить лишние суммы, создав учетную запись, а затем совершив снятие средств в течение одной секунды. Таким образом, депозит в 500 биткойнов может привести к добыче 2500 биткойнов.

В течение нескольких дней он создал около девяти учетных записей пользователей и совершил 140 транзакций.

Прокурор США Дамиан Уильямс из Южного округа Нью-Йорка объяснил поимку Чжуна «современным отслеживанием криптовалюты и старой доброй работой полиции».

В пятницу федеральный судья освободил Чжун под залог в размере 310 000 долларов». ***(David Parera. Feds Announce Silk Road Cryptocurrency Haul // Information Security Media Group, Corp. (https://www.govinfosecurity.com/feds-announce-silk-road-cryptocurrency-haul-a-20431). 07.11.2022).***

***

«Федеральна поліція Австралії (AFP) визначила групу «слабко пов'язаних» кіберзлочинців, що базуються в Росії, як тих, хто стояв за кібератакою на страхову компанію Medibank.

Комісар AFP Ріс Кершоу сказав, що агентству вдалося встановити особи хакерів, але він не назвав їх.

Кершоу зазначив, що AFP проведе переговори з російськими правоохоронними органами щодо кіберзлочинців.

Тим часом слідчі прочісують інтернет та «темне павутиння», вишукуючи людей, які отримують доступ до інформації та намагаються отримати з неї вигоду.

«Зараз час для всіх австралійців, суспільства, бізнесу та правоохоронних органів згуртуватися і не давати цим злочинцям тієї слави, якої вони прагнуть», — сказав Кершоу.

«Кіберзлочинність — це злом і проникнення 21 століття, а особиста інформація використовується як валюта».

Кершоу підтвердив, що політика уряду не виправдовує виплату викупу, бо будь-який викуп, маленький чи великий, «підживлює бізнес-модель кіберзлочинності».

Прем'єр-міністр Ентоні Албанезе раніше у п'ятницю заявив, що Москва має бути притягнута до відповідальності за злочинний акт.

«Річ у тому, що країна, звідки виходять ці атаки, також має бути притягнута до відповідальності за огидні атаки та розголошення інформації, включаючи дуже приватну та особисту інформацію».

Оприлюднення даних відбулося після того, як Medibank оголосив, що не поступатиметься вимогам кіберхакерів про викуп після того, як в результаті кібератаки в жовтні принаймні 9,7 мільйона його клієнтів отримали доступ до даних, включаючи повні імена, дати народження, номери телефонів, медичні номери та адреси.

«Ґрунтуючись на великій консультації, яку ми отримали від експертів з кіберзлочинності, ми вважаємо, що ймовірність того, що виплата викупу забезпечить повернення даних наших клієнтів і запобігатиме їх публікації, дуже мала», — заявив у понеділок клієнтам головний виконавчий директор Medibank Девід Кочкар.

«Насправді, виплата може мати зворотний ефект і спонукати злочинця безпосередньо вимагати гроші у наших клієнтів, і є велика ймовірність, що виплата поставить більше людей у небезпечне становище, зробивши Австралію більшою мішенню».

«Саме з цих причин ми вирішили, що не платитимемо викуп», — сказав він.

Компанія заявила, що це рішення також відповідає рекомендаціям уряду Австралії…» ***(Австралія: за зломом даних Medibank стоїть російська група хакерів // The Epoch Times (https://www.epochtimes.com.ua/novyny-svitu/avstraliya-za-zlomom-danyh-medibank-stoyit-rosiyska-grupa-hakeriv-video-147498). 12.11.2022).***

***

«Яньцзюнь Сюй — первый экстрадированный офицер китайской разведки, осужденный в США за попытки кражи интеллектуальной собственности.

Федеральный суд в Цинциннати в среду приговорил первого экстрадированного офицера китайской разведки к 20 годам тюремного заключения,

укрепив план Министерства юстиции по преследованию цифровых угроз национальной безопасности.

42-летний Янцзюнь Сюй был признан виновным по пунктам обвинения в сговоре с целью совершения экономического шпионажа, сговоре с целью совершения торгового хищения, попытке экономического шпионажа и попытке кражи коммерческой тайны.

В пресс-релизе, в котором объявляется об осуждении Сюй, указывается, что Сюй от имени правительства Китая связался с сотрудниками американских авиационных компаний, чтобы отправиться в Китай, где он способствовал сбору конфиденциальной информации компании. Композитный модуль вентилятора авиационного двигателя, запатентованный General Electric Aviation, был специально нацелен на кражу интеллектуальной собственности.

Как бывший высокопоставленный офицер разведки в Министерстве государственной безопасности Китая, Сюй использовал псевдонимы, чтобы скрыть свою личность и ввести в заблуждение сотрудников авиации США для поездки в Китай под предлогом чтения лекции в университете.

«Это дело посылает четкий сигнал: мы будем привлекать к ответственности любого, кто попытается украсть американские коммерческие секреты», — заявил прокурор США Кеннет Паркер из Южного округа штата Огайо. «Сюй сговорился украсть американскую науку и технологии. Благодаря усердной работе ФБР, GE Aviation и нашей судебной группы он проведет десятилетия в федеральной тюрьме».

Приговор Сюй — это последняя глава в растущей напряженности между США и Китаем, особенно в области конфиденциальности данных и передовых технологий. Чиновники юстиции утверждают, что схема была реализована с помощью китайских авиационных компаний.

«Этот случай — лишь последний пример продолжающихся атак китайского правительства на экономическую безопасность США — и, соответственно, на нашу национальную безопасность», — заявил директор ФБР Кристофер Рэй. «Китайское правительство поручило офицеру своей разведывательной службы украсть коммерческие секреты США, чтобы оно могло продвигать свои собственные усилия в области коммерческой и военной авиации за счет американской компании. Это наглое действие показывает, что китайское правительство не остановится ни перед чем, чтобы вывести наши компании из бизнеса в ущерб американским рабочим».

Как только сотрудники американской авиации сообщили об инциденте, сотрудники ФБР перехватили связь с Сюй, выдав себя за сотрудников авиации, имеющих доступ к конфиденциальной информации о конструкции.

В апреле 2018 года Сюй отправился в Бельгию под впечатлением, что он встретится с сотрудником американской авиации, путешествующим с запатентованными технологиями, где он был арестован агентами ФБР.

«Пока китайское правительство продолжает нарушать наши законы и угрожать американской промышленности и институтам, ФБР будет работать со своими партнерами по всему миру, чтобы привлечь виновных к ответственности», — сказал Рэй.

Ранее в сентябре сообщник Сюй Цзи Чаоцюнь был осужден по аналогичным обвинениям в шпионаже». ***(Alexandra Kelley. Yanjun Xu is the first extradited Chinese***

intelligence officer to be sentenced in the U.S., convicted of attempts to steal intellectual property // Nextgov (https://www.nextgov.com/technology-news/2022/11/extradited-chinese-national-sentenced-espionage-charges/379861/). 17.11.2022).

***

«…Сотрудники правоохранительных органов из 27 стран Интерпола объединили свои усилия в рамках Африканской операции по борьбе с киберпреступностью на всем континенте.

На фоне огромных финансовых потерь, понесенных компаниями, предприятиями и частными лицами, в ходе четырехмесячной операции (с июля по ноябрь 2022 г.) сотрудники правоохранительных органов выявляли, расследовали и пресекали киберпреступления посредством скоординированных правоохранительных действий с использованием платформ, инструментов и каналов Интерпола в тесном контакте. сотрудничество с АФРИПОЛ.

Координируемая из командного центра Интерпола в Кигали, Руанда, операция была направлена на устранение пособников киберпреступности.

Среди основных моментов эксплуатации:

11 человек были арестованы, один подозреваемый был связан с жестоким обращением с детьми, а 10 других были связаны с мошенничеством и мошенничеством на сумму 800 000 долларов США, которые оказали влияние на жертв во всем мире.

Власти Эритреи закрыли рынок даркнета, на котором продавались хакерские инструменты и компоненты киберпреступности как услуги.

В Камеруне было раскрыто несколько дел о мошенничестве с криптовалютой, в том числе одно с предполагаемым финансовым ущербом для жертвы в размере более 8 миллионов франков КФА.

Танзания вернула более 150 000 долларов денег жертв по делам о нарушении прав на данные и авторских правах.

Были предприняты действия против более чем 200 000 элементов вредоносной киберинфраструктуры, которые способствуют совершению киберпреступлений в Африканском регионе. Это включало демонтаж и очистку вредоносной инфраструктуры, связанной с активностью ботнета, а также распространение среди потенциальных жертв массовых фишинговых сообщений, спама и вымогательства в Интернете (например, мошенничества с романтическими отношениями, банковского мошенничества и кражи данных).

Страны-участницы смогли улучшить свою собственную национальную кибербезопасность, исправив уязвимости сети и очистив поврежденные правительственные веб-сайты, а также защитив уязвимую критически важную инфраструктуру, тем самым снизив риск потенциально катастрофических атак.

Расследования были основаны на данных, предоставленных партнерами Интерпола из частного сектора, включая British Telecom, Институт киберзащиты, Fortinet FortiGuard Labs, Group-IB, Kaspersky, Unit 42-Palo Alto Networks, Shadowserver и Trend Micro.

Эта информация также способствовала разработке 28 отчетов Интерпола о киберактивности, в которых освещались различные угрозы и виды преступной

деятельности, а также излагались рекомендуемые действия, которые должны быть предприняты национальными властями.

Участвующие следователи работали в своих странах в сотрудничестве с национальными группами реагирования на кибер-экстренные ситуации, интернет-провайдерами и хостинг-провайдерами, которые были уведомлены о потенциальной уязвимости в их сетевой инфраструктуре в пределах их юрисдикции.

Это сотрудничество оказалось очень успешным: 80% выявленных интернет-провайдеров обратились к правоохранительным органам, чтобы снизить риски, выявить слабые места в своей инфраструктуре и уведомить клиентов.

Из участвующих стран 18 признали группы реагирования на кибер-аварийные ситуации (CERT), все из которых активно сотрудничают с правоохранительными органами и интернет-провайдерами. Между этими организациями были заключены соглашения для формализации будущих ответов.

Координационная группа Интерпола в Кигали оказывала поддержку в режиме реального времени, а следователи из стран-участниц использовали безопасную совместную платформу для операций Интерпола по борьбе с киберпреступностью, чтобы сообщать друг другу о прогрессе, обмениваться разведывательными данными и получать поддержку.

Операция Cyber Surge не только впервые объединила многие африканские страны-члены в рамках единой операции по борьбе с киберпреступностью, но также помогла укрепить доверие и установить ценные рабочие отношения между ними и с другими партнерами.

Операции предшествовало двухнедельное учебное мероприятие в Кигали, Руанда, которое охватило расследования как киберпреступлений, так и криптовалют. Курс, проведенный в 23 правоохранительных органах из 22 африканских стран, дал участникам знания и навыки, необходимые для самой Операции, и позволит им предпринимать активные и устойчивые действия в будущем.

Обобщающая встреча, проведенная на Маврикии в конце ноября, позволила странам-членам поделиться успехами, обсудить проблемы и определить области для улучшения.

Деятельность Cyber Surge также привела к принятию новых законодательных протоколов и созданию ряда департаментов по борьбе с киберпреступностью в странах-членах, что будет способствовать дальнейшему снижению воздействия киберпреступности и защите сообществ в регионе.

Операция по борьбе с киберпреступностью в Африке координировалась Управлением Интерпола по борьбе с киберпреступностью и Программой поддержки Интерпола для Африканского союза (ISPA) в сотрудничестве с AFRIPOL.

Операция и связанные с ней мероприятия финансировались Министерством иностранных дел Великобритании по делам Содружества и развития и Федеральным министерством иностранных дел Германии в рамках их постоянной поддержки Интерпола и АФРИПОЛ». ***(International Operation Cracks Down on Cyber Criminals Across Africa // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/international-operation-cracks-down-on-cyber-criminals-across-africa/). 26.11.2022).***

***

«Услуги веб-сайта позволяли тем, кто зарегистрировался и оплатил услугу, анонимно совершать поддельные звонки, отправлять записанные сообщения и перехватывать одноразовые пароли.

Судебные и правоохранительные органы в Европе, Австралии, США, Украине и Канаде закрыли веб-сайт, который позволял мошенникам выдавать себя за доверенные корпорации или контакты для доступа к конфиденциальной информации жертв. Этот тип киберпреступления известен как «спуфинг». Считается, что веб-сайт нанес ущерб во всем мире, который оценивается в более чем 120 миллионов долларов.

В результате скоординированных действий, возглавляемых Соединенным Королевством и поддерживаемых Европолом и Евроюстом, были арестованы 142 подозреваемых, в том числе главный администратор веб-сайта.

Услуги веб-сайта позволяли тем, кто зарегистрировался и оплатил услугу, анонимно совершать поддельные звонки, отправлять записанные сообщения и перехватывать одноразовые пароли. Пользователи могли выдавать себя за бесконечное количество организаций (таких как банки, розничные компании и государственные учреждения) для получения финансовой выгоды и значительных потерь для жертв.

В ходе международной скоординированной акции, проведенной в ноябре этого года, по всему миру были арестованы 142 пользователя и администратора веб-сайта. Главный администратор сайта был арестован в Великобритании 6 ноября. 8 ноября сайт и сервер были конфискованы и отключены властями США и Украины.

Дело было открыто в Евроюсте в октябре 2021 года по запросу властей Великобритании. Национальные власти десяти стран, включая государства-члены Европейского союза и третьи страны, поддержали расследование. Агентство сыграло ключевую роль в содействии трансграничному судебному сотрудничеству между всеми вовлеченными сторонами. Евроюст провел два координационных совещания для координации национальных расследований и подготовки к действиям.

По запросу Соединенного Королевства Европол начал поддерживать дело ранее тем же летом (август 2021 г.). С тех пор Европейский центр по борьбе с киберпреступностью (EC3) Европола обеспечивает непрерывное развитие разведданных для национальных следователей через Совместную оперативную группу по борьбе с киберпреступностью (J-CAT). Кроме того, EC3 предоставила правоохранительным органам безопасную платформу для обмена большими пакетами доказательств. В рамках своей аналитической работы Европол смог выявить дополнительных пользователей сервиса iSpoof, ряд из которых уже был известен своей причастностью к другим громким расследованиям киберпреступлений на европейском уровне.

Следующие органы приняли участие или поддержали это расследование:

Австралия: Австралийская федеральная полиция

Канада: Королевская канадская конная полиция - Группа по расследованию киберпреступлений федеральной полиции Торонто

Франция: Подразделение по борьбе с киберпреступностью – PPO Paris; Правоохранительные органы: C3N - Национальная жандармерия

Германия: Bundeskriminalamt (Федеральное управление уголовной полиции) — Отдел по борьбе с киберпреступностью и Генеральная прокуратура в Бамберге — Баварское центральное управление по расследованию киберпреступлений

Ирландия: An Garda Síochána

Литва: Генеральная прокуратура Литовской Республики; Бюро криминальной полиции Литвы

Нидерланды: Группа по борьбе с киберпреступностью Midden-Nederland и прокуратура Midden-Nederland

Украина: Департамент киберполиции Национальной полиции Украины

Соединенное Королевство: Столичная полицейская служба (подразделение по борьбе с киберпреступностью), полиция лондонского Сити и Королевская прокуратура.

США: Федеральное бюро расследований – Питтсбургский отдел; Секретная служба США - полевой офис в Питтсбурге; и прокуратура США Западного округа Пенсильвании» ***(142 Arrests in Action Against Criminal Website that Offered Spoofing Services // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/142-arrests-in-action-against-criminal-website-that-offered-spoofing-services/). 26.11.2022).***

***

«Европол объявил об аресте гражданина России и Канады, связанного с атаками программы-вымогателя LockBit на объекты критической инфраструктуры и крупные промышленные группы.

Арест 26 октября последовал за многомесячным расследованием, проведенным Европейским центром киберпреступности (EC3) под руководством Национальной жандармерии Франции при содействии Канадской королевской канадской конной полиции (RCMP) и Федерального бюро расследований США (ФБР).

Власти сообщили, что они изъяли восемь компьютеров, 32 внешних жестких диска, два единицы огнестрельного оружия и криптовалюту на сумму около 400 000 евро из дома подозреваемого в Канаде.

Предполагаемый оператор программы-вымогателя LockBit, арестованный в Канаде, был «дорогой» целью

33-летний Михаил Васильев из Брэдфорда, Онтарио, Канада, считался важной целью в операции по вымогательству из-за его предполагаемой причастности к громким атакам с использованием программ-вымогателей. Правоохранительные органы заявили, что Васильев был известен тем, что требовал крупных выкупов от 5 до 70 миллионов евро (от 5,1 до 71,4 миллиона долларов).

Тем не менее, подозреваемый, скорее всего, будет активным партнером, использующим инфраструктуру LockBit для вымогателей как услуги (RaaS) для компрометации жертв с целью получения комиссионных после выплаты выкупа. Таким образом, его арест не повлияет на основную операцию программы-

вымогателя LockBit, хотя и уменьшит количество успешных атак со стороны опытных аффилированных лиц.

Сбор улик против оператора программы-вымогателя LockBit

В августе 2022 года канадские власти провели обыск в доме подозреваемого и обнаружили различные улики, которые привели к его аресту.

Доказательства включали чаты между подозреваемым и службой поддержки программы-вымогателя LockBit «LockBitSupp», в которой ему инструктировали о развертывании шкафчика LockBit для Linux/ESXi. Кроме того, они получили снимки экрана компьютера жертвы с именами пользователей и паролями для различных платформ. Они также обнаружили файл под названием TARGETLIST, содержащий имена прошлых и потенциальных жертв, в том числе компаний, которые пострадали от атаки программы-вымогателя LockBit в 2021 году. Другие важные доказательства включают исходный код программы, которая может шифровать данные, и ноутбук, подключенный к управлению LockBit. панель.

Судебные документы, увиденные 10 ноября, показывают, что Министерство юстиции США (Министерство юстиции) предъявило Васильеву обвинение. В настоящее время он ожидает экстрадиции в США, чтобы ответить за международные преступления.

33-летнему мужчине будет предъявлено обвинение в заговоре с целью умышленного повреждения защищенных компьютеров и передачи требований о выкупе, и ему грозит до пяти лет тюрьмы и штраф в размере 250 000 долларов или в два раза больше дохода от киберпреступления, если он больше.

Заместитель генерального прокурора Лиза О. Монако заявила, что арест Васильева стал результатом двух с половиной лет расследования программы-вымогателя LockBit и многолетнего опыта ФБР в борьбе с киберпреступностью.

Продолжающиеся аресты операторов программ-вымогателей

Европол сообщил, что двое его сообщников были арестованы в Украине в 2021 году в рамках другой операции. Дуэт был обвинен, среди прочего, в отмывании доходов от киберпреступлений. Тем не менее, многонациональное правоохранительное агентство не смогло раскрыть больше деталей, чтобы сохранить оперативную целостность.

Точно так же власти Украины ранее арестовали других членов групп вымогателей Clop и Egregor во время операции.

В октябре 2021 года Европол объявил об аресте 12 подозреваемых из различных групп вымогателей, включая Dharma, LockerGoga и MegaCortex, жертвами которых стали более 1800 человек из 71 страны.

Быстрый успех программы-вымогателя LockBit в сфере киберпреступности

Операция вымогателя LockBit началась в 2019 году, а его действия по программе-вымогателю были запущены в 2021 году. С тех пор группа вымогателей LockBit стала главным действующим лицом продвинутых постоянных угроз, ответственным за половину всех атак программ-вымогателей в 2022 году.

Согласно уголовному иску, поданному в Окружной суд США в Нью-Джерси, операция программы-вымогателя LockBit затронула более 1000 жертв в Соединенных Штатах и во всем мире. Международная операция по вымогательству

принесла киберпреступникам десятки миллионов долларов в виде выкупа от своих жертв после требования более 100 миллионов долларов.

Жертвами программы-вымогателя LockBit являются ИТ-консалтинговый гигант Accenture, который был скомпрометирован в августе 2021 года с украденными шестью терабайтами данных и требованием выкупа в размере 50 миллионов долларов, немецкий производитель автозапчастей Continental и британская железнодорожная служба Merseyrail. Другие включают технологического гиганта Foxconn, поставщика NHS Advanced и предполагаемую кражу данных французской аэрокосмической компании Thales». ***(Alicia Hope. Europol Arrested a "High Value" Russian-Canadian LockBit Ransomware Operator for Extradition to the US // CPO Magazine (https://www.cpomagazine.com/cyber-security/europol-arrested-a-high-value-russian-canadian-lockbit-ransomware-operator-for-extradition-to-the-us/). 17.11.2022).***

***

«Служба онлайн-спуфинга iSpoof была ликвидирована после расследования международных правоохранительных органов, в результате которого также были арестованы 146 человек, в том числе подозреваемый организатор операции.

Более сотни таких арестов, включая арест лидера платформы, были произведены столичной полицией Лондона.

iSpoof предлагал киберпреступникам так называемые «спуфинговые» серверы, которые позволяли им маскировать свои телефонные номера номером, принадлежащим доверенной организации, создавая у жертв впечатление, будто им звонил их банк.

Эта подделка номера телефона позволила мошенникам проводить социальную инженерию, фишинг и мошенничество с «службой поддержки банка», кража денег, учетных данных банковского счета и одноразовых кодов.

«Услуги веб-сайта позволили тем, кто зарегистрировался и оплатил услугу, анонимно совершать поддельные звонки, отправлять записанные сообщения и перехватывать одноразовые пароли», — заявил в четверг Европол.

«Пользователи могли выдавать себя за бесконечное количество организаций (таких как банки, розничные компании и государственные учреждения) для получения финансовой выгоды и значительных потерь для жертв».

Согласно заявлению столичной полиции, с июня 2021 года по июль 2022 года с помощью iSpoof было совершено 10 миллионов мошеннических звонков по всему миру.

Европол сообщает, что iSpoof нанес около 120 000 000 долларов убытков, а операторы сервиса получили предполагаемую прибыль в размере 3 850 000 долларов за последние 16 месяцев.

Раскрытие iSpoof

Департамент по борьбе с киберпреступностью голландской полиции заявил, что обнаружил серверы с iSpoof в Алмере, маленьком городке недалеко от Амстердама, во время расследования мошенничества со службой поддержки банка.

Это привело к новому расследованию, посвященному сервису, в результате которого было обнаружено местонахождение оператора iSpoof в Лондоне. Затем они проинформировали Скотленд-Ярд, который начал собственное тщательное расследование в отношении подозреваемого.

Затем полиция Нидерландов прослушивала серверы в Алмере и собирала информацию о том, как работает сервис и кто им пользуется.

Полиция Великобритании сообщает, что тайная операция по отслеживанию iSpoof началась в июне 2021 года, что помогло правоохранительным органам составить карту преступной сети.

Европол подключился в августе 2021 года, чтобы помочь полиции Великобритании собрать доказательства и разведданные от партнеров по правоохранительным органам со всего мира.

В рамках своей аналитической работы Европол смог выявить дополнительных пользователей сервиса iSpoof, ряд из которых уже был известен своей причастностью к другим громким расследованиям киберпреступлений на европейском уровне. — Европол

Владелец iSpoof был арестован в воскресенье, 6 ноября 2022 г., в Восточном Лондоне, а известные веб-сайты iSpoof, такие как ispoof.cc и ispoof.me, были конфискованы.

Также были арестованы администраторы серверов в Алмере, двое мужчин 19 и 22 лет. Полиция Нидерландов подчеркивает, что в настоящее время они деанонимизируют больше пользователей сервиса на основании доказательств, собранных с захваченных серверов.

После удаления iSpoof пользователям службы с форумов даркнета было рекомендовано «выбросить все». ***(Bill Toulas. 'iSpoof' service dismantled, main operator and 145 users arrested // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ispoof-service-dismantled-main-operator-and-145-users-arrested/). 24.11.2022).***

***

«Впервые Министерство юстиции США конфисковало семь доменов, на которых размещались веб-сайты, связанные с мошенничеством с «разделкой свиней», где мошенники обманом заставляют жертв романтических афер инвестировать в криптовалюту через поддельные инвестиционные платформы.

Список изъятых доменов включает simexcbr.com, simexlua.com, simexwim.com, simexarts.com, simexrue.com, simexvtn.com и simexbiz.com, все они подделывают домен, используемый Сингапурской международной валютной биржей (SIMEX).

Мошенничество с разделкой свиней, происходящее из Азии, распространилось по всему миру после того, как мошенники криптовалюты поняли, что пользователи приложений для знакомств и сайтов социальных сетей («свиньи») становятся легкой добычей после завоевания доверия с использованием различных тактик социальной инженерии.

Попавшись на крючок, жертвами занимаются другие члены сети киберпреступников, которые также управляют мошенническими криптовалютными инвестиционными платформами.

После того, как мошенники попросили инвестировать и перевести средства с помощью предоплаченных карт, банковских переводов и платежей в криптовалюте на кошельки, контролируемые злоумышленниками, или через банкоматы, они закрыли свой поддельный крипто-инвестиционный портал и исчезли с деньгами жертв.

Пятеро пострадавших потеряли более 10 миллионов долларов

Как сообщило Министерство юстиции США в пресс-релизе на этой неделе, мошенническая сеть, использовавшая семь изъятых доменов, обманом заставила пятерых жертв перевести более 10 миллионов долларов на депозитные адреса в криптовалюте, которые были немедленно опустошены мошенниками.

Например, в августе 2022 года одна из жертв рассказала следователям, что один из мошенников, который вышел на связь через мобильные мессенджеры LINE и WeChat, продвигал криптовалютную инвестиционную платформу с использованием домена simexlua.com.

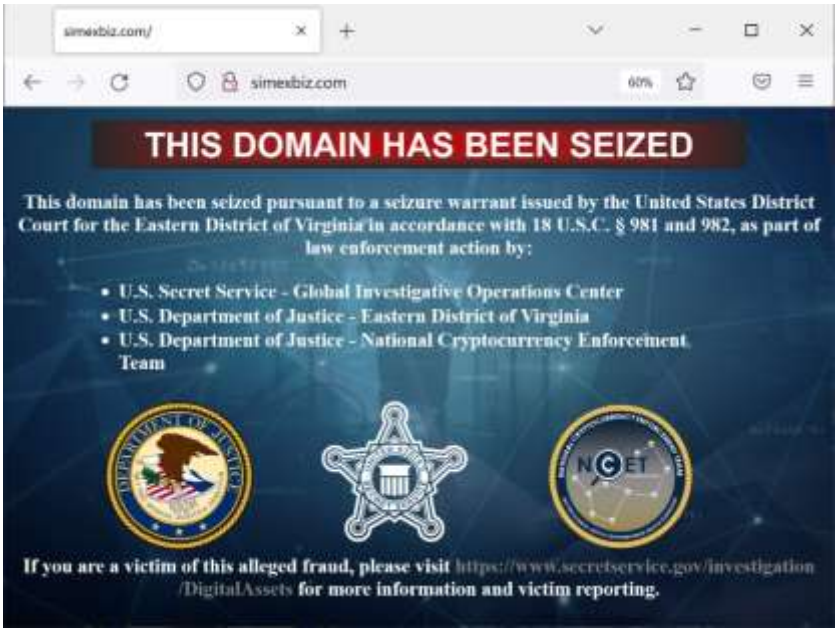
После того, как в мае 2022 года их обманом заставили установить поддельное инвестиционное приложение и первоначально сделать небольшую инвестицию в размере 400 долларов США, жертвы перевели около 9,6 миллионов долларов США в монетах (USDC) на адрес депозита, предоставленный мошенниками.

Согласно письменным показаниям, опубликованным в среду, мошенники также отправляли уведомления о «торговой прибыли» через мошенническое приложение после каждого депозита, чтобы жертва «инвестировала».

Когда жертва попыталась вывести часть фальшивой прибыли на общую сумму более 7 миллионов долларов за фальшивые оповещения в приложении, мошенники запросили дополнительные платежи в виде «налогов», «сборов» и «гарантийных депозитов», чтобы доказать, что они «не причастен к любому противоправному поведению».

«Согласно судебным протоколам, по крайней мере, с мая по август 2022 года мошенники привлекли пять жертв в Соединенных Штатах, используя семь конфискованных доменов, которые все были поддельными доменами Сингапурской международной валютной биржи», — говорится в сообщении Министерства юстиции.

«После того, как жертвы переводили инвестиции на депозитные адреса, которые мошенники предоставили через семь захваченных доменных имен, средства жертв были немедленно переведены через многочисленные частные кошельки и обменные сервисы, чтобы скрыть источник средств. жертвы потеряли более 10 миллионов долларов».



Баннер захвата simexbiz.com (BleepingComputer)

ФБР предупреждает криптовалютных инвесторов

ФБР также недавно предупредило о мошенничестве с разделкой свиней, подчеркнув, что это становится очень прибыльной схемой во всем мире, когда киберпреступники крадут постоянно растущее количество криптовалюты у ничего не подозревающих инвесторов.

«Многие жертвы сообщают о том, что им было приказано совершать электронные переводы на зарубежные счета или покупать большие суммы по предоплаченным картам», — предупредило ФБР в прошлом месяце.

«Использование криптовалюты и криптовалютных банкоматов также является новым методом оплаты. Индивидуальные потери, связанные с этими схемами, варьировались от десятков тысяч до миллионов долларов».

ФБР также поделилось списком некоторых красных флажков, которые должны дать инвесторам понять, что они являются целью мошенничества с «разделкой свиней»:

С вами связывается давно потерянный контакт или незнакомец в социальных сетях.

URL-адрес инвестиционной платформы не совпадает с официальным сайтом популярного рынка/биржи криптовалют, но очень похож (опечатка).

Загруженное инвестиционное приложение выдает предупреждения о том, что ему не доверяют, при запуске в Windows, или ваш антивирус помечает его как потенциально опасное.

Инвестиционная возможность звучит слишком хорошо, чтобы быть правдой.

Тем, кто подозревает, что они могли стать жертвой такого мошенничества, настоятельно рекомендуется подать отчет в центр жалоб на преступления IC3.gov или обратиться по адресу CryptoFraud@SecretService.gov». ***(Sergiu Gatlan. U.S. govt seizes domains used in 'pig butchering' scams // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/us-govt-seizes-domains-used-in-pig-butchering-scams/). 24.11.2022).***

***

«В прошлом месяце в Женеве был арестован Вячеслав Игоревич Пенчуков, также известный как Танк и один из лидеров печально известной киберпреступной группировки JabberZeus.

Федеральное управление юстиции Швейцарии (FOJ) заявило, что Пенчуков был арестован в прошлом месяце и ожидает экстрадиции в США, хотя он все еще может обжаловать решение FOJ.

«По приказу Федерального управления юстиции (FOJ) и на основании запроса об экстрадиции из США гражданин Украины был арестован в кантоне Женева 23 октября 2022 года и задержан в ожидании экстрадиции», — сообщили BleepingComputer в швейцарской прокуратуре.

«Власти США обвиняют преследуемого в вымогательстве, банковском мошенничестве и краже личных данных, в том числе. В ходе слушаний 24 октября 2022 года лицо не дало согласия на его экстрадицию в США в порядке упрощенного производства.

«После завершения формальной процедуры экстрадиции Федеральное управление юстиции приняло решение о его экстрадиции в США 15 ноября 2022 года. Решение Министерства юстиции может быть обжаловано в Федеральном уголовном суде Швейцарии или, соответственно, в Верховном суде Швейцарии».

Журналист по кибербезопасности Брайан Кребс впервые сообщил, что Пенчуков был арестован во время поездки в Женеву на встречу с женой.

Плакат о розыске JABBERZEUS (ФБР)

От кражи банковских счетов до программ-вымогателей

Министерство юстиции США впервые предъявило Пенчукову обвинение в 2012 году, обвинив его в причастности к заговору с целью кражи миллионов долларов с использованием номеров банковских счетов, паролей, личных идентификационных номеров и другой конфиденциальной информации, похищенной с помощью печально известного вредоносного ПО Zeus.

Несколько источников ранее сообщали BleepingComputer, что Пенчуков также был одним из руководителей операций по вымогательству Maze и Egregor.

Программа-вымогатель Maze популяризировала атаки с двойным вымогательством, когда злоумышленники также похищали данные и использовали

их в качестве дополнительного рычага, чтобы заставить жертв заплатить выкуп. Позже Maze был переименован в операции «Эгрегор» и «Сехмет», чтобы уклониться от правоохранительных органов.

BleepingComputer также сообщили, что он был среди подозреваемых, арестованных в январе 2021 года украинской полицией после международной правоохранительной операции, направленной против членов банды вымогателей Egregor.

Однако, согласно отчету Кребса, ему удалось избежать судебного преследования с помощью своих политических связей, в том числе с покойным сыном бывшего президента Украины Виктора Януковича.

Как один из лидеров киберпреступной группировки JabberZeus, Пенчуков управлял украденными банковскими реквизитами и денежными мулами, которые переводили деньги со счетов жертв на счета, контролируемые киберпреступниками.

Вместе с восемью другими подозреваемыми ему было предъявлено обвинение в сговоре с целью участия в «рэкете, сговоре с целью совершения компьютерного мошенничества и кражи личных данных, краже личных данных при отягчающих обстоятельствах и множественных случаях банковского мошенничества».

Двое его сообщников, граждане Украины Евгений Кулибаба и Юрий Коноваленко, признали себя виновными в ноябре 2014 года после экстрадиции из Великобритании и были приговорены к двум годам и десяти месяцам лишения свободы в мае 2015 года». ***(Sergiu Gatlan. Suspected Zeus cybercrime ring leader 'Tank' arrested by Swiss police // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/suspected-zeus-cybercrime-ring-leader-tank-arrested-by-swiss-police/). 16.11.2022).***

***

«Интерпол объявил об аресте денег и виртуальных активов на сумму 130 000 000 миллионов долларов, связанных с различными киберпреступлениями и операциями по отмыванию денег.

Операция правоохранительных органов под кодовым названием «HAECHI III» продолжалась с 28 июня по 23 ноября 2022 года, что позволило Интерполу арестовать почти тысячу подозреваемых.

«Всего в результате операции было задержано 975 человек и раскрыто более 1600 дел», — говорится в сообщении Интерпола.

«Кроме того, было заблокировано почти 2800 банковских счетов и счетов с виртуальными активами, связанных с незаконными доходами от финансовых преступлений в Интернете».

Типы киберпреступлений, в результате которых была получена указанная сумма, включают мошенничество с романтическими отношениями, голосовой фишинг, секс-вымогательство, мошенничество с инвестициями и отмывание денег, связанное с незаконными азартными играми в Интернете.

В результате этой акции Интерпол также сгенерировал 95 уведомлений и рассылок, а также обнаружил шестнадцать новых тенденций в области преступности, которые помогут правоохранительным органам по всему миру принимать более целенаправленные меры против киберпреступников.

Новые тенденции включают в себя разновидности мошенничества с романтическими отношениями и мошенничества с инвестициями, которые злоумышленники постоянно совершенствуют, чтобы сохранить элемент новизны.

Кроме того, Интерпол отметил рост количества зашифрованных приложений для обмена сообщениями, используемых мошенниками для обмена информацией с жертвами в инвестиционных схемах.

Два основных момента операции HAECHI III:

Арест двух корейцев в Греции и Италии, которые присвоили 29 100 000 долларов у 2000 жертв в Корее.

Арест членов базирующейся в Индии преступной группировки, которые выдавали себя за сотрудников Интерпола, чтобы звонить жертвам и обманом заставлять их отправлять им 159 000 долларов в криптовалюте.

В заявлении Интерпола также подчеркивается эффективность его нового механизма протокола быстрого реагирования (ARRP) по борьбе с отмыванием денег, который впервые был протестирован в ходе предыдущей операции агентства под кодовым названием «Операция Шакал».

Благодаря ARRP, ирландской компании, которая стала жертвой компрометации деловой электронной почты (BEC), ей было возвращено 1 250 000 миллионов долларов. Это была общая сумма, которую компания потеряла из-за мошенников BEC, которую ARRP помог отследить и изъять.

С января 2022 года, когда начался этап пилотного тестирования ARRP, этот инструмент помог вернуть 120 000 000 долларов доходов от киберпреступлений». ***(Bill Toulas. Interpol seized $130 million from cybercriminals worldwide // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/interpol-seized-130-million-from-cybercriminals-worldwide/). 24.11.2022).***

***

«Двое эстонских граждан были арестованы в Эстонии в воскресенье после того, как в США им было предъявлено обвинение в использовании масштабной схемы криптовалюты Понци, которая привела к убыткам на сумму более 575 миллионов долларов.

Подсудимые, 37-летние Сергей Потапенко и Иван Турыгин, обвиняются в обмане сотен тысяч жертв вместе с четырьмя другими сообщниками, проживающими в Эстонии, Беларуси и Швейцарии в период с декабря 2013 года по август 2019 года.

Утверждается, что они направляли средства жертв через сложную сеть подставных компаний, банковских счетов, сервисов виртуальных активов и криптовалютных кошельков, предназначенных для отмывания денег.

Начиная с декабря 2013 года они управляли компанией HashCoins OÜ, которая импортировала и собирала оборудование для майнинга криптовалюты других компаний вместо того, чтобы производить собственное, как рекламировалось.

После того, как не удалось доставить оплаченное заранее оборудование и избежать возврата платежей, ответчики обманом заставили клиентов, которые уже заплатили за оборудование для майнинга, подписаться на контракты на удаленный

майнинг (облачный майнинг) через новый сервис майнинга криптовалюты, который они назвали HashFlare (запущенный в феврале 2015 г.).

Согласно обвинительному заключению, тем, кто согласился на эту схему, было обещано получить «права по контрактам на добычу полезных ископаемых, дающие заказчику право на процент прибыли» от объединенной удаленной операции по добыче полезных ископаемых.

Вместо этого Потапенко и Турогин использовали HashFlare как крупную финансовую пирамиду, где возврат валюты и балансы были мошенническими.

«Чтобы скрыть этот факт, когда инвесторы подавали запросы на вывод своих доходов от майнинга, ответчики либо сопротивлялись осуществлению платежей, либо расплачивались с инвесторами, используя виртуальную валюту, которую ответчики просто покупали на открытом рынке, а не валюту, генерируемую настоящими операциями майнинга», — заявил суд. документы говорят.

Революционный цифровой крипто-банкинг

И последнее, но не менее важное: они также основали новую компанию в Эстонии под названием Polybius Foundation OÜ (он же Polybius Bank) и пригласили потенциальных инвесторов финансировать проекты посредством «первичного размещения монет» (ICO) в обмен на виртуальные токены, известные как токены Polybius (PLBT) как часть «настоящей революции в мире цифрового криптобанкинга».

Спустя две недели в пресс-релизе Polybius утверждалось, что «ICO привлекло около 17 миллионов долларов от более чем 14 250 участников», из них более 6 миллионов долларов менее чем за три дня, что «соответствует требованиям для получения европейской банковской лицензии».

В общей сложности им удалось привлечь более $31 млн от сторонних инвесторов (согласно расследованию ФБР HashFlare), средства, которые были переведены на банковские счета ответчиков и кошельки виртуальной валюты вместо того, чтобы использоваться для финансирования Polybius Bank. Они никогда не выплачивали инвесторам никаких дивидендов и никогда не создавали банк.

Вместо этого средства, полученные мошенническим путем, были использованы для покупки не менее 75 объектов недвижимости, роскошных автомобилей, пополнения их криптовалютных кошельков и инвестирования в тысячи машин для майнинга криптовалюты.

«Размер и масштабы предполагаемой схемы поистине поразительны. Эти ответчики воспользовались как привлекательностью криптовалюты, так и тайной, связанной с добычей криптовалюты, чтобы совершить огромную схему Понци», — сказал прокурор США Ник Браун.

«Они заманивали инвесторов ложными заявлениями, а затем расплачивались с ранними инвесторами деньгами тех, кто инвестировал позже. Эстонские власти работают над тем, чтобы арестовать и ограничить эти активы и получить прибыль от этих преступлений».

Им предъявлено обвинение по 16 пунктам обвинения в мошенничестве с использованием электронных средств, по одному пункту обвинения в сговоре с целью отмывания денег и в сговоре с целью совершения мошенничества с использованием электронных средств.

В случае признания виновным каждому из них грозит максимальное наказание в виде 20 лет лишения свободы». ***(Sergiu Gatlan. Two Estonians arrested for running $575M crypto Ponzi scheme // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/two-estonians-arrested-for-running-575m-crypto-ponzi-scheme/). 21.11.2022).***

***

«Национальная полиция Испании ликвидировала киберпреступную организацию, которая использовала поддельные инвестиционные сайты для хищения более 12,3 млн евро (12,8 млн долларов США) у 300 жертв по всей Европе.

Вредоносные кампании включали создание фальшивых сайтов для инвестирования в криптовалюту, внешне похожих на известные законные платформы.

Затем злоумышленники отмывали деньги, украденные у жертв, переводя их из испанских банков в иностранные финансовые организации, где, как надеялись преступники, они были вне поля зрения властей или возможности их отслеживания.

Расследование правоохранительных органов Испании было начато после того, как законный представитель одной из выдающихся финансовых групп сообщил об этом в полицию.

В ходе операции шесть членов киберпреступной организации были арестованы в Мадриде и Барселоне, и им будут предъявлены обвинения в подозрении в мошенничестве, отмывании денег и узурпации семейного положения.

Мошеннический процесс

Злоумышленники создали сеть фальшивых банковских сайтов, используя технику типосквоттинга, заключающуюся в регистрации доменов, аналогичных официальным сайтам реальных, выдающихся банков.

Изменив символ или поменяв местами две буквы, домены могут по-прежнему казаться небрежным посетителям подлинными.

Как правило, жертвы попадают на эти сайты, переходя по ссылкам, встроенным в фишинговые электронные письма, и именно так расформированная испанская банда также привлекала трафик на свои сайты.

В то время как жертвы группы угроз происходят из нескольких стран Европы, большинство поддельных веб-сайтов были нацелены на французов и, следовательно, выдавали себя за французские финансовые учреждения.

Жертв заставляли думать, что они вкладывали деньги в эти веб-сайты, но на самом деле их депозиты переводились непосредственно на банковские счета преступной группировки.

«Метод мошенничества, используемый преступной группой, заключался в том, чтобы предлагать любому потенциальному клиенту через мошеннические веб-сайты возможность проведения различных финансовых операций, таких как: заключение контрактов на инвестиционные продукты (переменный доход, фьючерсы и криптовалюты) и заключение контрактов на финансовые продукты» - Испанская полиция

Украденные средства были переведены на банковские счета мошенников в Испании, Португалии, Польше и Франции, а затем переведены в иностранные организации для отмывания денег. После попыток скрыть след денег средства в конечном итоге были возвращены на испанские счета.

Полицейское расследование установило, что общая сумма денег, отправленных в конечный пункт назначения преступной группы, составила 12 345 731 евро». ***(Bill Toulas. Spanish police dismantle operation that made €12M via investment scams // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/spanish-police-dismantle-operation-that-made-12m-via-investment-scams/). 29.11.2022).***

***

«Громадянин російської федерації Олексій Смірнов разом мешканцями України організували потужне хакерське угрупування, котре займається вимаганням коштів завдяки викраденню грошей та інформації. Як з'ясувала редакція 368.media зловмисники працюють з 2015 року. У групи є багато різних назв. У Мінюсті США їх маркують як FIN7. Проте у світі вони більш відомі як Carbanak чи Cobalt (також Anunak, Navigator Group).

Олексій СмірновЦя злочинна організація налічує понад 70 осіб, об'єднаних у підрозділи та групи. Деякі були хакерами, інші розробляли зловмисне програмне забезпечення, встановлене на комп'ютерах, а треті створювали шкідливі електронні листи, які змусили жертв заразити системи їхніх компаній. Зловмисники брали участь у надскладній кампанії зловмисного ПО для атаки на сотні американських компаній, переважно в ресторанному бізнесі, індустрії ігор та готельному бізнесі. FIN7 зламав тисячі комп'ютерних систем і викрав мільйони номерів кредитних і дебетових карток клієнтів, які використовувалися або продавалися з метою отримання прибутку.

Хакери ретельно створювали повідомлення електронної пошти, які здавалися б законними для співробітників компанії, і супроводжував листи телефонними дзвінками, призначеними для подальшої легітимізації. Після відкриття та активації вкладеного файлу FIN7 використовував би адаптовану версію відомого зловмисного програмного забезпечення Carbanak на додаток до арсеналу інших інструментів для отримання доступу та викрадення даних платіжних карток для клієнтів компанії. З 2015 року багато вкрадених номерів платіжних карток пропонувалися для продажу через підпільні онлайн-ринки.

Лише в Сполучених Штатах FIN7 успішно зламала комп'ютерні мережі у всіх 50 штатах і окрузі Колумбія, викравши понад 20 млн записів карток клієнтів із понад 6,5 тис. індивідуальних торгових терміналів у понад 3,6 тис. окремих бізнес-локаціях. Додаткові вторгнення відбулися за кордоном, зокрема у Великій Британії, Австралії та Франції. Збитки склали понад 1 млрд доларів.

Перші вироки

У 2018 році у США арештували трьох громадян України за підозрою в причетності до угруповання— Федіра Гладиря, Дмитра Федоріва та Андрія Колпакова.

Гладир спочатку приєднався до FIN7 через підставну компанію під назвою Combi Security — фальшиву компанію з кібербезпеки, яка мала фальшивий веб-сайт і не мала законних клієнтів. Гладир працював системним адміністратором FIN7, який, серед іншого, відігравав центральну роль у зборі інформації про викрадені платіжні картки, нагляді за хакерами FIN7 та обслуговуванні складної мережі серверів, які FIN7 використовував для атак і контролю комп'ютерів жертв. Гладир також контролював зашифровані канали зв'язку організації. Гладиря у 2018 році заарештували в Дрездені та екстрадували до Сієтла. У 2021 році його засудили 10 років позбавлення волі та виплаті 2,5 млн доларів компенсації.

Андрія Колпакова, котрий виконував роль експерта з тестування на проникнення, засудили на сім років з виплатою компенсації у 2,5 млн доларів. Його затримали у Лепе, Іспанія та також екстрадували до США. Щодо Федоріва, то інформації про його вирок знайти не вдалося.

Також у грудні 2019 року під час весільної подорожі в аеропорту Бангкока затримали та доправили у США українця Дениса Ярмака. Він приймав участь у розробці фішингових електронних писем із шкідливим ПО, проникненням у мережу жертв і вилучення таких даних, як відомості про платіжну карту. Його у квітні 2022 року засудили до 5 років позбавлення волі.

У 2018 році затримали ще одного члена угрупування — лідера групи Carbanak Дениса Токаренко. Спочатку уроженець Магаданської області організував крадіжку коштів в російських банках. Він був оголошений у розшук і з'ясувалося — чоловік із 2013 року перебрався до Одеси, де отримав українське громадянство під прізвищем Катана. Чотири роки тому хакер із родиною переїхав до Іспанії на Плайя-де-Сан-Хуан. Місцевий суд відмовив у його видачі росії.

Зрештою, був затриманий лише навесні 2018 року. Як писала газета El Mundo, геній кіберзлочинності забув сплатити купівлю авто. За кілька місяців до арешту Денис за 70 тис. євро придбав машину, але так і не розрахувався. Продавець занепокоївся, і на початку березня заявив у поліцію. Копи з'явилися в дім Дениса, вважаючи, що мають справу зі звичайним боржником. І лише зіставивши дані, усвідомили, що перед ними людина, яка перебуває у розшуку за дистанційне спустошення банкоматів та банківських рахунків у всьому світі. Як би там не було, хакера було затримано, а його головну зброю – ноутбук – конфісковано. На ньому правоохоронці виявили сліди багатства чоловіка: 15 тисяч біткоїнів — близько 162 млн доларів за курсом на той момент. У 2021 році Токаренко засудило до 4,5 років позбавлення волі.

Об'єднання діє

Незважаючи на резонансні затримання та вироки, группа FIN7 та її філіали продовжують свою справу. Так влітку цього року Держспецзв'язку України в особі команди CERT-UA повідомила, що у документах від імені податкової служби міститься небезпечний вірус, який відкриває доступ до комп'ютера жертви. Зловмисники надсилають жертвам листи з темою «Повідомлення про несплату податку» та пропонується ознайомитися із сумою боргу у прикріпленому документі. При відкритті на пристрій завантажується HTML-файл і виконується JavaScript-код (CVE-2022-30190), який встановлює та запускає вірусну програму Cobalt Strike

Beacon. Як відзначають фахівці, таким чином хакери працюють уже тривалий час, їхня активність відстежується за ідентифікатором UAC-0098.

Згідно з даними редакції, мережу хакерів очолює той самий Олексій Смірнов, який зараз мешкає у Іспанії. Смірнов — людина-привид. Однак редакція 368.media знайшла його коріння у Московській області. В 2013 році суд міста Клин розглядав справу про хуліганство зі зброєю, котре вчинил Смірнов. Перебуваючи у нетверезому стані на вулиці біля автобусної зупинки, чоловік зажадав від оточуючих дати йому цигарку. Отримавши бажане, він кинув її в бік людини. З хуліганських міркувань Смірнов дістав із внутрішньої кишені куртки пневматичний пістолет. Смірнов зробив у бік потерпілого один постріл, потрапивши у скляну частину зупинки. Йому повідомили про підозру по ч. 1 ст. 213 КК рф. У суді Смирнов дійшов згоди з потерпілими, тому справу закрили.

У Смірнова є багато помічників в Україні. Наприклад, зараз триває суд над киянином Андрієм Дюговським. Він є обвинуваченим по ч. 2 ст. 189, ч. 2 ст. 361 КК у справі № 42020101010000132, яку відкрили у 2020 році. Слідство вважає, що Дюговський вимагав від компаній гроші за розблокування діяльності комп`ютерних мереж, які попередньо будуть заблоковані ним із використанням шкідливого програмного забезпечення (Egregor Ransomware). Він разом зі спільниками за допомогою програмного забезпечення Cobalt Strike розпочали опрацювання комп’ютерних мереж логістичної компанії GEFCO (Париж, Франція), які заблокували 20 вересня 2020 року. Окрім цього їхньою жертвою стала логістичная компанія Hempt Bros, Inc. (штат Пенсильванія, США).

Ще одна справа № 12020000000001091 ч. 2 ст. 361, ч. 2 ст. 209 КК досі розслідується головним слідчим управлінням Національної поліції. Там мова йде про хакерські атаки на сервера корейських компаній у період з 13 по 22 лютого 2019 року за допомогою Flawed Ammyy RAT та програми-вимагача Clop. До цього причетні власники ТОВ «Ярд Девелопмент» — Ігор Котенко, Олександр Підвальний та Борис Мазур. За даними слідства саме Котенко має електронні гаманці Binance та Huobi на який надходять кошти, отримані через програми-вимагачі Russian apt та bulletproof (обмінники з високим ризиком).

Сам Котенко родом з Санкт-Петербургу. Наприкінці листопада 2020 року вилетів через аеропорт «Бориспіль» до республіки Білорусь. Він має тісні зв’язки з іншим хакером, який в більшості часу проживає у м. Москва, де здійснює злочинну діяльність пов`язану з шкідливим програмним забезпечення Cobalt Strike.

Органи досудового розслідування також вказують, що представники біржі Binance надали електронні гаманці і підв`язані до них пошти, які запитувані правоохоронними органами інших держав, а саме поліцією Іспанії, Секретною службою США, Федеральним бюро розслідувань, поліцією Кореї, поліцією Німеччини і Податковою службою США. Злочинець займається легалізацією коштів через придбання та реєстрацію на себе та на підставних осіб, зокрема, на своїх близьких родичів і знайомих, велику кількість об`єктів нерухомого та рухомого майна. До легалізації також причетна компанія «Трансекспресавто», де трійця чоловіків була засновниками. До теперішного часу вироків по справі досі немає.

Хакерське угрупування продовжує свою роботу. Смірнов створив новий шахрайській проект у сфері блокчейну A4 finance. Це типова шахрайська схема про яку ми раніше писали.

Керівником проекту він призначив людину, котра представляється Олександром Фельдманом. Він є офіційним CEO проєкту у сфері блокчейну A4 finance. Фельдман з Кривого Рог та живе у Сумах і буває Києві. Його родичка Дарина Проценко, яка відкрила фірми у Латвіі та на Маршалових островах, керує усіма рахунками. До речі, ніякого Фельмана не існує — це недостовірне прізвище Олександра Северенчука, про яку редакція 368.media розповідала тут.

Раніше уряд США поклав відповідальність за атаки на ланцюжок поставок на російську ФСБ, яке використовує інструмент Cobalt Strike у своєму наборі інструментів як мінімум з 2018 року. Згідно з даними американської Cybersecurity and Infrastructure Security Agency встановлено, що на спецслужби рф працює BERSERK BEAR (also known as Crouching Yeti, Dragonfly, Energetic Bear, and Temp.Isotope). Вона, згідно з галузевими звітами, історично націлені на організації в Західній Європі та Північній Америці, включаючи державні, місцеві, племінні та територіальні (SLTT) організації, а також організації сектора енергетики, транспортних систем і оборонно-промислової бази (DIB). Ця група також націлилася на сектор систем водопостачання та водовідведення та інші об’єкти критичної інфраструктури.

Щодо шкідливого забезпечення Cobalt, то наразі його використовує російська група WIZARD SPIDER. Це група кіберзлочинців, яка розробляє зловмисне програмне забезпечення TrickBot і програми-вимагачі Conti. Історично склалося так, що група платила заробітну плату тим, хто розгортає програми-вимагачі (іменовані афілійованими особами), деякі з яких потім можуть отримати частку доходів від успішної атаки програм-вимагачів. На додаток до TrickBot, помітні початкові вектори доступу та стійкості для афілійованих учасників включають Emotet, Cobalt Strike, підводне фішинг і вкрадені або слабкі облікові дані протоколу віддаленого робочого столу (RDP).

Після отримання доступу афілійовані особи WIZARD SPIDER покладалися на різні загальнодоступні та законні інструменти для полегшення попередніх етапів життєвого циклу атаки перед розгортанням програми-вимагача Conti. WIZARD SPIDER пообіцяв підтримку російському уряду та погрожував організаціям критичної інфраструктури країн, які, як вважають, здійснюють кібератаки чи війну проти російського уряду. Пізніше вони переглянули цю обіцянку та погрожували помстою за ймовірні напади на російський народ. Організації жертв Conti охоплюють різні галузі, зокрема будівництво та проектування, юридичні та професійні послуги, виробництво та роздрібну торгівлю. Крім того, філії WIZARD SPIDER розгорнули програмне забезпечення-вимагач Conti проти мереж охорони здоров’я США та мереж швидкого реагування». ***(Андрей Вышинский. Росіянин організував потужне хакерське угрупування з українців // 368.media (https://368.media/2022/11/07/rosiyanin-organizuvav-potuzhne-hakerske-ugrupuvannya-z-ukrayintsiv-2/). 07.11.2022).***

***

«Министерство юстиции США обвинило человека с двойным российско-канадским гражданством в участии в одной из самых масштабных операций с применением программы-вымогателя.

33-летний Михаил Васильев был арестован в среду в Канаде и ожидает экстрадиции в США, сообщил Минюст.

Согласно судебным документам, Васильев, который живет в Брэдфорде, провинция Онтарио, якобы участвовал в кампании с применением вредоносной программы LockBit.

В ходе подобных атак киберпреступники используют такие программы, как LockBit для шифрования данных на компьютере жертвы, после чего требуют выкуп в обмен на ключ для разблокировки файлов.

Арест можно рассматривать как победу Минюста.

Киберпреступников редко арестовывают и привлекают к ответственности, поскольку они часто действуют вне досягаемости американских правоохранительных органов в странах, с которыми у США нет договоров об экстрадиции». ***(В Канаде арестован россиянин, обвиняемый в причастности к кибератакам с программой-вымогателем // Голос Америки (https://www.golosameriki.com/a/canadian-national-arrested/6829992.html). 11.11.2022).***

***

Технічні аспекти кібербезпеки

«Internet Security Research Group (ISRG), некоммерческая организация, стоящая за Let's Encrypt, сообщает, что открытый центр сертификации (CA) выпустил в этом году свой трехмиллиардный сертификат.

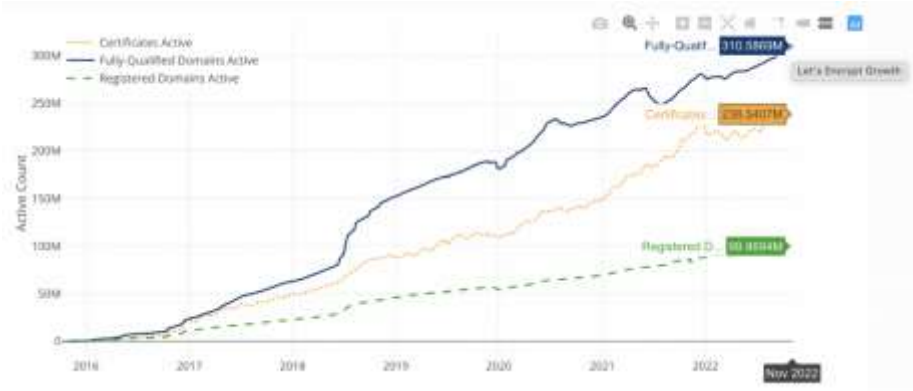
Let’s Encrypt бесплатно предоставляет веб-сайтам цифровые сертификаты X.509, необходимые для включения HTTPS (SSL/TLS) и зашифрованной связи, с сентября 2015 года, когда был выпущен первый сертификат для домена helloworld.letsencrypt.org.

Начиная с августа 2018 года Let's Encrypt напрямую доверяют все основные браузеры и операционные системы, а также все основные программы корневых сертификатов (в том числе от Microsoft, Google, Apple, Mozilla, Oracle и Blackberry).

Бесплатный и автоматизированный ЦС позволяет любому владельцу домена получить доверенный сертификат без каких-либо затрат. В настоящее время CA заявляет, что выпускает миллионы таких писем ежедневно.

Как сообщила сегодня ISRG, это позволило ей достичь нового рекорда в этом году, поскольку в настоящее время она предоставляет услуги более чем 300 миллионам веб-сайтов.

«По состоянию на 1 ноября 2022 года Let’s Encrypt предоставляет TLS более чем 309 миллионам доменов с помощью 239 миллионов активных сертификатов. Использование Let’s Encrypt выросло более чем на 33 миллиона доменов в 2022 году», — говорится сегодня в годовом отчете ISRG за 2022 год.



Давайте зашифруем статистику роста (Let's Encrypt)

Чтобы получить представление о масштабах работы ЦС и о том, что подтолкнуло его команду разработчиков к дальнейшей автоматизации выдачи и продления сертификатов, в начале марта 2020 года ему пришлось отозвать более 3 миллионов сертификатов из-за ошибки в его программном обеспечении для проверки и выдачи доменов.

Это число составило примерно 2,6% от примерно 116 миллионов активных сертификатов, предоставленных веб-сайтам по всему миру.

Почти два года спустя, в январе 2022 года, Let’s Encrypt объявила об отзыве миллионов активных сертификатов SSL/TLS, что затронет примерно 1% всех активных сертификатов Let’s Encrypt.

«С тех пор мы разработали спецификацию для автоматизации сигналов обновления сертификатов, чтобы наши подписчики могли обрабатывать события отзыва/обновления так же легко, как и получать сертификаты (это происходит автоматически в фоновом режиме!), — сказал Джош. Аас, исполнительный директор ISRG.

«Эта спецификация проходит через процесс стандартизации IETF, чтобы вся экосистема могла извлечь выгоду, и мы планируем вскоре развернуть ее в рабочей среде Let's Encrypt».

Сегодняшнее рекордное объявление было сделано после того, как в феврале 2020 года Let’s Encrypt сообщила, что выпустила 1 миллиард сертификатов, менее чем через три года после того, как объявила об отметке в 100 миллионов». ***(Sergiu Gatlan. Let’s Encrypt issued over 3 billion certificates, securing 309M sites for free // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/let-s-encrypt-issued-over-3-billion-certificates-securing-309m-sites-for-free/). 29.11.2022).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Microsoft обнаружила рост использования нулевых дней китайскими хакерами за последний год

Первый год действия китайского закона, требующего обязательного раскрытия правительству отчетов об уязвимостях, совпадает с периодом увеличения масштабов использования программ нулевого дня хакерами, поддерживаемыми Пекином.

Это вывод компьютерного гиганта Microsoft, который говорит, что положение об обязательном раскрытии информации «может позволить элементам в китайском правительстве накапливать сообщения об уязвимостях для их использования в качестве оружия».

Требование о раскрытии информации вступило в силу 1 сентября 2021 года в рамках более крупного Закона о безопасности данных, ужесточающего правила обработки китайских данных. Поставщики, обнаружившие уязвимости, должны сообщить о них властям в течение двух дней для включения в национальную базу данных уязвимостей Китая.

Американская компания по кибербезопасности Recorded Future опубликовала исследование в 2017 году, в котором раскрывается официальный процесс, возглавляемый ведущим агентством гражданской разведки, Министерством государственной безопасности, который, вероятно, оценивает сообщения о высокой уязвимости к угрозам на предмет их оперативной полезности перед публикацией в CNNVD.

Еще до того, как закон вступил в силу, китайская хакерская группа, которую Microsoft назвала Hafnium, использовала четыре эксплойта нулевого дня для взлома локальных версий Microsoft Exchange Server. Официальный представитель Белого дома заявил, что жертв насчитывалось около 140 000 человек; в их число входили исследователи инфекционных заболеваний, юридические фирмы, высшие учебные заведения, оборонные подрядчики, аналитические центры и неправительственные организации. Соединенные Штаты и их союзники в июле назвали атаки частью модели «безответственного и дестабилизирующего поведения в киберпространстве».

По словам Microsoft, позже в 2021 году китайские хакеры обнаружили еще одну атаку нулевого дня на Exchange. CVE-2021-42321 появилась во время Tianfu Cup, международного саммита по кибербезопасности и соревнований по хакерству, которые состоялись 16 и 17 октября 2021 года в Чэнду, Китай. Менее чем через неделю кто-то уже использовал его в дикой природе.

Вычислительный гигант также приписывает разработку и развертывание четырех дополнительных нулевых дней китайским государственным субъектам, включая недостаток SolarWinds, CVE-2021-35211; две уязвимости в ПО службы ИТ-поддержки от Zoho, CVE-2021-40539 и CVE-2021-44077; и ошибка в Atlassian Confluence Server and Data Center, CVE-2022-26134.

По словам Microsoft, в среднем требуется 14 дней, чтобы эксплойт появился в дикой природе после публичного раскрытия уязвимости. Шестьдесят дней спустя, как правило, появляется доказательство концепции, а через 120 дней уязвимость будет включена в автоматизированные инструменты уязвимости и эксплуатации». ***(Prajeet Nair. China Likely Amasses 0-Days Via Vulnerability Disclosure Law // Information Security Media Group, Corp. (https://www.govinfosecurity.com/china-likely-amasses-0-days-via-vulnerability-disclosure-law-a-20436). 08.11.2022).***

***

«Поддерживаемые государством хакеры, возможно, китайцы, использовали нулевые дни

Microsoft исправила пару уязвимостей нулевого дня Exchange, о которых стало известно в конце сентября и которые, как известно, использовались злоумышленниками с признаками китайского происхождения.

Первый недостаток — это уязвимость подделки запросов на стороне сервера, которая позволяет злоумышленникам получить доступ к внутренним серверам, которых у них не было бы в противном случае. Вторая уязвимость допускает удаленное выполнение кода при активированной удаленной оболочке PowerShell. Злоумышленники могут использовать первую уязвимость, чтобы активировать вторую. Это, соответственно, CVE-2022-41040 и CVE-2022-41082, и вместе они известны как ProxyNotShell из-за их сходства с тремя уязвимостями Exchange 2021 года, вместе известными как ProxyShell.

В отличие от ProxyShell, эти недостатки требуют аутентификации злоумышленника в Exchange. ProxyNotShell влияет на выпуски Microsoft Exchange 2013, 2016 и 2019, и Microsoft заявляет, что организациям, которые разгрузили локальные серверы в пользу Exchange Online, не нужно предпринимать никаких действий.

В сентябрьском анализе Microsoft заявила, что наблюдала менее 10 организаций, пострадавших от атак ProxyNotShell, и выразила «со средней степенью уверенности», что злоумышленником, вероятно, была организация, спонсируемая государством. В то время он рекомендовал меры по смягчению последствий, включая ограничение доступа к PowerShell. Теперь компания заявляет, что системные администраторы должны установить патч.

Вьетнамская компания по кибербезопасности GTSC первой сообщила об уязвимостях, заявив, что злоумышленники оставляли запутанные веб-оболочки для последующего использования в качестве бэкдора. GTSC поднял вопрос о том, что хакеры имеют китайское происхождение, отметив, что они используют AntSword — «активный китайский кроссплатформенный инструмент администрирования веб-сайтов с открытым исходным кодом, который поддерживает управление веб-оболочкой», кодирование веб-оболочки упрощенными китайскими иероглифами и, вероятно, использование веб-оболочки China Chopper.

Microsoft не приписывает деятелю национального государства, хотя недавно обвинила Пекин в вероятном накоплении запасов нулевого дня с целью использования их в качестве оружия для хакерских атак, поддерживаемых государством». ***(David Parera. Microsoft Patches ProxyNotShell Exchange Vulnerabilities // Information Security Media Group, Corp. (https://www.govinfosecurity.com/microsoft-patches-proxynotshell-exchange-vulnerabilities-a-20441). 09.11.2022).***

***

«Исследователи Checkmarx Security обнаружили уязвимость GitHub, которая позволяет злоумышленникам захватывать и отравлять тысячи пакетов с открытым исходным кодом с миллионами пользователей.

Эта уязвимость, получившая название RepoJacking (захват репозитория), затрагивает функцию прекращения использования пространства имен GitHub, которая защищает репозитории переименованных учетных записей пользователей.

Эксперты по безопасности предупредили, что критическая уязвимость может привести к широкомасштабным атакам на цепочки поставок программного обеспечения, затрагивающим миллионы пользователей.

Уязвимость GitHub позволяет пользователям восстанавливать переименованные учетные записи

Команда Checkmarx Supply Chain Security обнаружила, что логическая ошибка позволяет пользователю GitHub воссоздать репозиторий GitHub, идентичный репозиторию в переименованной учетной записи.

GitHub попытался предотвратить этот эксплойт, пометив репозиторий с более чем 100 клонами как удаленный в момент переименования его учетной записи пользователя. Однако платформа позволяет пользователям восстанавливать переименованные имена пользователей, хотя и не позволяет им создавать репозитории, соответствующие тем, которые ранее существовали под этим именем пользователя.

По словам исследователей, GitHub рассматривает комбинации имени пользователя и имени репозитория как пространство имен, которое нельзя восстановить. Однако злоумышленники обнаружили способ обойти это ограничение, создав соответствующие репозитории под другим именем пользователя и переименовав свою учетную запись в целевое переименованное имя пользователя.

«Репозиторий GitHub уязвим для реподжекинга, когда его создатель решил переименовать свое имя пользователя, в то время как старое имя пользователя доступно для регистрации. Это означает, что злоумышленники могут создать новую учетную запись GitHub с той же комбинацией, которая соответствует URL-адресу старого репозитория, используемого существующими пользователями», — написали исследователи безопасности Checkmarx Йоссеф Харуш и Авиад Гершон.

Перехват пространства имен не позволяет инструменту выхода из эксплуатации GitHub перенаправлять пользователей на новый URL-адрес переименованного пакета с открытым исходным кодом. Вместо этого он передает их непосредственно в восстановленный пакет под контролем злоумышленника.

Уязвимость GitHub затрагивает более 10 000 пакетов с открытым исходным кодом

Исследователи Checkmarx обнаружили, что уязвимость GitHub затронула все переименованные имена пользователей в GitHub и репозиториях в большинстве менеджеров пакетов. На данный момент фирма по кибербезопасности идентифицировала более 10 000 пакетов в менеджерах пакетов Go, Swift и Packigist, использующих переименованные имена пользователей.

В основном затронуты языки программирования, которые извлекают пакеты с открытым исходным кодом непосредственно из системы управления версиями,

такие как PHP, и пользователи, которые добавили в закладки переименованные пакеты с открытым исходным кодом.

Исследователи предупредили, что уязвимость GitHub приведет к захвату популярных пакетов кода и распространению вредоносных кодов среди миллионов пользователей, что приведет к массовым атакам на цепочку поставок.

«Практический смысл этого заключается в том, что тысячи пакетов могут быть немедленно захвачены и запущены для доставки вредоносного кода миллионам пользователей и множеству приложений», — написали они.

«Тысячи проектов с миллионами конечных пользователей полагаются на библиотеки с открытым исходным кодом и репозитории кода, что делает репозитории очень привлекательной мишенью для злоумышленников», — сказал Майк Паркин, старший технический инженер Vulcan Cyber.

Checkmarx обнаружил уязвимость GitHub в ноябре 2021 года и сообщил об этом материнской компании Microsoft. В марте 2022 года GitHub сообщил об устранении уязвимости. Однако в мае 2022 года Checkmarx обнаружил, что функция передачи репозитория все еще может быть использована, и поделился своими выводами с GitHub.

Однако GitHub еще не исправил уязвимость на момент раскрытия информации. Компания по безопасности приложений из Атланты, штат Джорджия, стала публичной после того, как «безрассудный исследователь безопасности» похитил три пакета с открытым исходным кодом, воспользовавшись популярным инструментом удаления пространства имен репозитория.

Checkmarx опубликовал инструмент Chainjacking для разработчиков Go, чтобы определить, используют ли они уязвимые пакеты с открытым исходным кодом в своих проектах. Фирма по безопасности также создала систему мониторинга для обнаружения попыток взлома уязвимости GitHub до тех пор, пока платформа не примет необходимые меры.

Тим Макки, главный специалист по стратегии безопасности Synopsys Cybersecurity Research Center, сказал, что пользователи GitHub должны определить окончание срока службы для поддерживаемых ими пакетов с открытым исходным кодом.

«Это включает в себя наличие доверенных лиц в качестве владельцев или групповых учетных записей и определение преемника GitHub — в дополнение к публикации явных заявлений об окончании срока службы или устаревании».

Макки посоветовал разработчикам не полагаться на историческую популярность пакета исходного кода при запуске нового проекта. Вместо этого они должны подтвердить, что репозиторий исправен и активно поддерживается.

«Здоровые проекты можно определить с помощью GitHub Insights проекта, а также по данным Code Contributors и Code Frequency. Если проект популярен, а активность ограничена или активность ограничена горсткой участников, то этот проект не так здоров, как может указывать его популярность».

По словам Макки, злоумышленники предпочитают нездоровые, но популярные пакеты с открытым исходным кодом.

Мелисса Бишопинг, директор по исследованиям Endpoint Security в Tanium, сказала, что распространенность пакетов с открытым исходным кодом и общих библиотек на предприятиях представляет наибольший риск повторного взлома.

«При разработке программного обеспечения важно проверять код в этих репозиториях, а также создавать собственный частный форк для работы (вместо извлечения из текущего общедоступного репозитория)», — сказала она». ***(Alicia Hope. GitHub Vulnerability Allows Hackers to Hijack Thousands of Popular Open-Source Packages // CPO Magazine (https://www.cpomagazine.com/cyber-security/github-vulnerability-allows-hackers-to-hijack-thousands-of-popular-open-source-packages/). 14.11.2022).***

***

«Усилия по каталогизации уязвимых систем для помощи в восстановлении; Включает элементы управления конфиденциальностью

Представители британской разведки говорят, что новый проект по сканированию британского Интернета на наличие уязвимых систем является частью усилий по повышению национального уровня кибербезопасности.

Национальный центр кибербезопасности — общедоступный компонент разведывательного агентства правительственных коммуникаций — раскрыл проект сканирования в своем блоге во вторник.

«Мы не пытаемся найти уязвимости в Великобритании для каких-то других гнусных целей. Мы начинаем с простых сканирований и будем постепенно увеличивать сложность сканирований, объясняя, что мы делаем», — написал Ян Леви, NCSC. технический директор.

Проект будет регулярно сканировать сетевые системы по всей Великобритании для обнаружения уязвимостей. Идея состоит в том, чтобы собирать данные для количественной оценки подверженности риску и реагировать на потрясения, такие как широко используемая уязвимость нулевого дня.

NCSC заявляет, что будет использовать облачные инструменты, которые подключаются к IP-адресам, назначенным scanner.scanning.service.ncsc.gov.uk. Конкретно 18.171.7.246 и 35.177.10.231.

Чтобы решить проблемы конфиденциальности, NCSC заявляет, что будет избегать сбора личной информации. Данные, полученные от пользователей, будут включать ответ HTTP, включая заголовки с веб-серверов. Для других служб он будет удерживать «данные, отправленные сервером сразу после установления соединения или действительного рукопожатия протокола».

Сетевые администраторы могут отказаться, отправив агентству свой IP-адрес по электронной почте.

Сканирование интернета на наличие уязвимостей, конечно, вряд ли можно назвать оригинальным занятием. Хакеры и компании, занимающиеся кибербезопасностью, молча делают это десятилетиями. В 2014 году исследователь кибербезопасности Роб Грэм представил инструмент, который он назвал masscan, способный сканировать весь Интернет за считанные минуты.

«Интернет довольно маленький, всего 4 миллиарда адресов», — сказал он участникам конференции Def Con в Лас-Вегасе в то время. «Вы найдете системы,

которые можно взломать, за считанные минуты». ***(Akshaya Asokan. UK NCSC Says Friendly Spooks Scanning British Internet // Information Security Media Group, Corp. (https://www.govinfosecurity.com/uk-ncsc-says-friendly-spooks-scanning-british-internet-a-20405). 03.11.2022).***

***

«Субъекты, связанные с иранским правительством, смогли использовать неисправленную уязвимость Log4Shell, которую Агентство по кибербезопасности и безопасности инфраструктуры попросило агентства устранить к концу 2021 года, в сети неназванного агентства.

Согласно совместному бюллетеню по кибербезопасности, опубликованному Агентством кибербезопасности и безопасности инфраструктуры и ФБР в среду, хакеры, спонсируемые правительством Ирана, смогли использовать неустраненную уязвимость в сети федерального агентства, чтобы скомпрометировать учетные данные пользователей и установить программное обеспечение для майнинга криптовалюты в своей системе.

CISA и ФБР заявили, что неназванная «федеральная гражданская организация исполнительной власти» была скомпрометирована «уже в феврале 2022 года». В бюллетене не приписывается нарушение какой-либо конкретной группе, кроме того, что оно было совершено «спонсируемыми иранским правительством субъектами [расширенной постоянной угрозы]». Но в бюллетене говорилось, что хакеры смогли использовать уязвимость Log4Shell — программную уязвимость в Log4j, популярной библиотеке журналов с открытым исходным кодом — на «неисправленном сервере VMware Horizon».

CISA заявила, что впервые узнала о взломе в апреле, когда провела анализ сети агентства с помощью EINSTEIN — «системы обнаружения вторжений в масштабах [федеральной гражданской исполнительной власти]» — и выявила «двунаправленный трафик между сетью и известный вредоносный IP-адрес, связанный с использованием уязвимости Log4Shell». CISA заявила, что с середины июня по середину июля 2022 года провела в агентстве «операцию по реагированию на инциденты», в ходе которой обнаружила «предполагаемую продвинутую постоянную активность угроз».

В бюллетене говорится, что злоумышленники «установили программное обеспечение для крипто-майнинга XMRig» в сети агентства, а также «имплантировали обратные прокси-серверы Ngrok на несколько хостов для обеспечения устойчивости». Хакеры также установили приложение с открытым исходным кодом Mimikatz для «сбора учетных данных» и создания «мошеннической учетной записи администратора домена».

Нарушение произошло всего через несколько месяцев после того, как в декабре 2021 года CISA издало экстренную директиву, требующую от федеральных агентств оценить свои сети на наличие уязвимости Log4Shell и «немедленно исправить эти системы или принять другие соответствующие меры по смягчению последствий». Директива предоставила агентствам до 17:00 23 декабря того же года, чтобы определить, затронуто ли их программное обеспечение уязвимостью, используя репозиторий GitHub, управляемый CISA, «чтобы определить,

присутствует ли Log4j в этих активах, и если да, то являются ли эти активы подвержены уязвимости». Агентствам также был дан крайний срок 28 декабря, чтобы отчитаться перед CISA обо «всем затронутом программном обеспечении», а также о шагах, которые они предприняли для устранения уязвимости.

«CISA издало эту экстренную директиву, чтобы побудить федеральные гражданские агентства принять меры для защиты своих сетей, сосредоточив внимание в первую очередь на устройствах с выходом в Интернет, которые представляют наибольший непосредственный риск», — заявила в то время директор CISA Джен Истерли. «CISA также настоятельно призывает все крупные и малые организации последовать примеру федерального правительства и предпринять аналогичные шаги для оценки своей сетевой безопасности и адаптации мер по смягчению последствий, изложенных в нашей директиве по чрезвычайным ситуациям».

Наряду с недавним советом по компрометации CISA также поделилась отчетом об анализе вредоносного ПО для программного обеспечения для майнинга криптовалюты XMRig, чтобы помочь пользователям и сетевым администраторам выявлять аналогичные вторжения в свои системы и защищаться от них.

«CISA и ФБР призывают все организации с уязвимыми системами VMware, которые не сразу применили доступные исправления или обходные пути, признать компрометацию и начать поиск угроз», — говорится в бюллетене». ***(Edward Graham. Iranian Hackers Compromised a Federal Agency's Network, CISA and FBI Say // Nextgov (https://www.nextgov.com/cybersecurity/2022/11/iranian-hackers-compromised-federal-agencys-network-cisa-and-fbi-say/379832/). 16.11.2022).***

***

«Федеральные агентства подчиняются обязательным оперативным директивам по устранению уязвимых мест безопасности в своем программном обеспечении, но успех усилий CISA зависит от сотрудничества поставщиков программного обеспечения.

Агентство по кибербезопасности и безопасности инфраструктуры в четверг выпустило набор документов, определяющих приоритетность устранения уязвимостей программного обеспечения агентствами и другими организациями. Но использование руководства в значительной степени зависит от поставщиков, предоставляющих информацию, необходимую для проведения такого процесса.

В своем блоге о «преобразовании ландшафта управления уязвимостями» исполнительный помощник директора CISA Эрик Гольдштейн призвал предприятия использовать «категоризацию уязвимостей для конкретных заинтересованных сторон» — процесс, впервые сформулированный CISA совместно с Институтом программной инженерии Университета Карнеги-Меллон, — для принятия решения о том, какая система ошибки, которые они должны исправить в первую очередь.

На агентства распространяется обязательная операционная директива о получении и рассмотрении отчетов об уязвимостях от исследователей безопасности в определенные сроки, и они решают, какие доказательства они могут потребовать от поставщиков программного обеспечения, подтверждающие безопасные методы

разработки, в соответствии с указом о повышении национальной кибербезопасности от мая 2021 года.

Гольдштейн отметил, что CISA использовала методологию SSVC при составлении своего каталога сотен известных уязвимостей, которые могут быть использованы агентствами, на которые также должны ссылаться агентства — в соответствии с другой обязательной операционной директивой — при применении структуры для устранения слабых мест, о которых они уже знают, в их предприятиях.

Но не все программные уязвимости хорошо известны — или зарегистрированы как распространенные уязвимости и риски, или CVE — в общедоступных базах данных. И в видении Гольдштейна для совершенствования методов управления уязвимостями использование методологии приоритезации SSVC является третьим в трехэтапном процессе.

«Во-первых, мы должны повысить автоматизацию управления уязвимостями, в том числе за счет расширения использования Common Security Advisory Framework. Во-вторых, мы должны облегчить организациям понимание того, подвержен ли данный продукт уязвимости, за счет повсеместного внедрения обмена уязвимостями», — сказал он, описывая первый и второй этапы.

Common Security Advisory Framework, или CSAF, — это машиночитаемый формат, который поставщики программного обеспечения могут использовать для информирования клиентов об уязвимостях, существующих в их коде. Обмен уязвимостями или VEX — это документ, который поставщик может использовать, чтобы объяснить, как они могли нейтрализовать определенные уязвимости, чтобы пользователям не приходилось беспокоиться о том, что они все еще присутствуют в их продуктах. Поставщик также может выделить наличие уязвимости с помощью VEX, чтобы пользователи могли расставить приоритеты в ее исправлении.

Гольдштейн отметил, что VEX может быть особенно полезен при использовании в тандеме со спецификацией программного обеспечения.

Распоряжение от мая 2021 года, изданное в ответ на взлом SolarWinds, было направлено на то, чтобы дать агентствам больше информации о приобретаемом ими программном обеспечении. Но выполнение заказа через Национальный институт стандартов и технологий и Управление управления и бюджета оставило на усмотрение самих агентств определять, должны ли они запрашивать у поставщиков доказательства, такие как SBOM, при рассмотрении своих покупок программного обеспечения.

Система приоритизации CISA, выпущенная для управления уязвимостями, инструктирует пользователей оценивать пять факторов: статус эксплуатации, техническое воздействие, автоматизацию, распространенность миссии и влияние на общественное благополучие.

CISA заявила, что работает в рамках Федеральной программы управления рисками и авторизацией Управления общих служб, чтобы заставить облачные сервисы внести свой вклад в устранение уязвимостей, но агентство по-прежнему несет ответственность за то, чтобы напрямую связываться с поставщиками, когда в их системах обнаруживаются ошибки». ***(Mariam Baksh. CISA Issues Vulnerability-Management Tools Dependent on Industry Action // Nextgov***

(https://www.nextgov.com/cybersecurity/2022/11/cisa-issues-vulnerability-management-tools-dependent-industry-action/379632/). 16.11.2022).

***

«Внедрение такой методологии, как SSVC, является важным шагом в развитии экосистемы управления уязвимостями.

CISA опубликовала руководство по специфической для заинтересованных сторон категоризации уязвимостей (SSVC) — методологии управления уязвимостями, которая оценивает уязвимости и определяет приоритеты усилий по исправлению на основе статуса эксплуатации, воздействия на безопасность и распространенности уязвимого продукта в отдельной системе.

Как указано в сообщении блога помощника исполнительного директора (EAD) Эрика Гольдштейна «Трансформация ландшафта управления уязвимостями», внедрение такой методологии, как SSVC, является важным шагом на пути развития экосистемы управления уязвимостями. Кроме того, в блоге подробно описаны усовершенствования, в том числе каталог известных эксплуатируемых уязвимостей (KEV) CISA, машиночитаемые рекомендации по безопасности Common Security Advisory Framework (CSAF) и обмен информацией об использовании уязвимостей (VEX), которые, используемые в сочетании с SSVC, уменьшат Субъектам оконных киберугроз приходится использовать сети.

CISA рекомендует организациям прочитать сообщение в блоге EAD Goldstein и использовать следующие ресурсы на веб-странице SSVC для улучшения своих процессов управления уязвимостями:

Дерево решений CISA SSVC

Руководство SSVC по использованию SSVC и дерева решений SSVC

Калькулятор SSVC для определения приоритетов реагирования на уязвимости в соответствующей среде организации…» ***(CISA Releases SSVC Methodology to Prioritize Vulnerabilities // Homeland Security Today (https://www.hstoday.us/federal-pages/dhs/cisa-releases-ssvc-methodology-to-prioritize-vulnerabilities/). 11.11.2022).***

***

«Интеграция новой технологии в систему 911 расширяет возможные векторы угроз и поверхности атаки системы.

Центры экстренной связи (ECC)/автоответчики общественной безопасности (PSAP) могут получить доступ к одностраничному справочному пособию с практическими шагами, которые они могут предпринять для повышения уровня кибербезопасности своей системы 911.

Две вещи, которые каждый центр 911 должен сделать для повышения кибербезопасности PDF-файл был разработан SAFECOM Агентства кибербезопасности и безопасности инфраструктуры и Национальным советом координаторов функциональной совместимости штата, потому что:

Для систем службы экстренной помощи требуется стабильная, безопасная и отказоустойчивая связь.

Кибер-уязвимости в системе 911 могут быть использованы преступниками или государственными угрозами.

Интеграция новой технологии в систему 911 расширяет возможные векторы угроз и поверхности атаки системы.

Документ настоятельно призывает все ECC/PSAP:

Проведите оценку киберрисков.

На основе результатов оценки кибер-рисков разработайте планы реагирования на кибер-инциденты и реагирования на уязвимости.

Чтобы помочь с этими рекомендациями, документ содержит определения для оценки кибер-рисков и планов реагирования на кибер-инциденты и кибер-уязвимости, а также содержит ссылки на дополнительные инструкции по их выполнению.

Также включены практические шаги, которые ECC/PSAP могут предпринять для поддержки своих усилий по планированию, например:

Выполнение планов.

Поддержание координации с заинтересованными сторонами, такими как их координатор по интероперабельности в масштабе штата.

Рассмотрение внедрения обнаружения и смягчения киберугроз, а также NG911 для расширенных возможностей безопасности…» ***(Action Steps to Enhance 911 System Cybersecurity // Homeland Security Today (https://www.hstoday.us/federal-pages/dhs/action-steps-to-enhance-911-system-cybersecurity/). 04.11.2022).***

***

«Microsoft и Google заявили, что около 70 процентов их уязвимостей связаны с проблемами безопасности памяти программного обеспечения.

Агентство национальной безопасности (АНБ) опубликовало руководство, призванное помочь разработчикам и операторам программного обеспечения предотвратить и смягчить проблемы с безопасностью памяти программного обеспечения, на которые приходится большая часть уязвимостей, которые можно использовать.

В информационном бюллетене по кибербезопасности «Безопасность памяти программного обеспечения» рассказывается, как злоумышленники могут использовать проблемы с плохим управлением памятью для доступа к конфиденциальной информации, обнародования несанкционированного выполнения кода и других негативных последствий.

«Проблемы управления памятью эксплуатировались десятилетиями и до сих пор слишком распространены, — сказал Нил Зиринг, технический директор по кибербезопасности. «Мы должны постоянно использовать безопасные для памяти языки и другие средства защиты при разработке программного обеспечения, чтобы устранить эти уязвимости от злоумышленников».

Microsoft и Google заявили, что около 70 процентов их уязвимостей связаны с проблемами безопасности памяти программного обеспечения. Плохое управление памятью также может привести к техническим проблемам, таким как неправильные результаты программы, ухудшение производительности программы с течением времени и сбои программы.

АНБ рекомендует организациям по возможности использовать безопасные для памяти языки и укреплять защиту с помощью средств защиты кода, таких как

параметры компилятора, параметры инструментов и конфигурации операционной системы…» ***(NSA Releases Guidance on How to Protect Against Software Memory Safety Issues // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/nsa-releases-guidance-on-how-to-protect-against-software-memory-safety-issues/). 11.11.2022).***

***

«Субъекты киберугроз воспользовались уязвимостью Log4Shell на неисправленном сервере VMware Horizon и установили программное обеспечение для крипто-майнинга XMRig.

С середины июня по середину июля 2022 года CISA провела операцию по реагированию на инциденты в организации Федеральной гражданской исполнительной власти (FCEB), где CISA обнаружила предполагаемую активность продвинутых постоянных угроз (APT). В ходе реагирования на инциденты CISA определила, что субъекты киберугроз использовали уязвимость Log4Shell на неисправленном сервере VMware Horizon, установили программное обеспечение для крипто-майнинга XMRig, переместились на контроллер домена (DC), скомпрометировали учетные данные, а затем внедрили обратные прокси-серверы Ngrok. на нескольких хостах для сохранения постоянства. CISA и Федеральное бюро расследований (ФБР) считают, что сеть FCEB была скомпрометирована спонсируемыми иранским правительством субъектами APT.

CISA и ФБР выпускают этот информационный бюллетень по кибербезопасности (CSA), в котором представлены тактики, методы и процедуры (TTP) подозреваемых иранских правительственных субъектов, а также индикаторы компрометации (IOC), чтобы помочь защитникам сети обнаруживать и защищаться от связанных компрометаций.

CISA и ФБР призывают все организации с уязвимыми системами VMware, которые не сразу применили доступные исправления или обходные пути, признать компрометацию и начать поиск угроз. Если на основе IOC или TTP, описанных в этом CSA, обнаруживается подозреваемый первоначальный доступ или компрометация, CISA и ФБР рекомендуют организациям допускать горизонтальное перемещение злоумышленников, исследовать подключенные системы (включая DC) и проверять привилегированные учетные записи. Все организации, независимо от выявленных признаков компрометации, должны применять рекомендации из раздела «Смягчение последствий» данного CSA для защиты от подобных злонамеренных действий в киберпространстве.

Для получения дополнительной информации о спонсируемой правительством Ирана вредоносной киберактивности в Иране см. веб-страницу CISA «Обзор и рекомендации по киберугрозам в Иране» и веб-страницу «Иранские угрозы» ФБР». ***(Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/iranian-government-sponsored-apt-actors-compromise-federal-network-deploy-crypto-miner-credential-harvester/). 18.11.2022).***

***

«Агентство национальной безопасности (АНБ) призвало разработчиков и операторов программного обеспечения перейти на безопасные для памяти языки и предотвратить проблемы с безопасностью памяти программного обеспечения, ответственные за большинство уязвимостей, которые можно использовать.

Согласно Информационному бюллетеню по кибербезопасности «Безопасность памяти программного обеспечения», злоумышленники могут использовать проблемы с плохим управлением памятью для доступа к конфиденциальным данным и выполнения незаконного кода, среди прочего.

Технический директор АНБ по кибербезопасности Нил Зиринг заявил, что проблемы с управлением памятью использовались десятилетиями и до сих пор распространены. «Мы должны последовательно использовать безопасные для памяти языки и другие средства защиты при разработке программного обеспечения, чтобы устранить эти недостатки от злоумышленников», — добавил он.

Технологические гиганты Microsoft и Google связывают 70% уязвимостей некоторых своих продуктов с проблемами безопасности программной памяти.

Слишком много свободы и гибкости в управлении памятью

АНБ обвинило в проблемах с эксплойтной памятью свободу и гибкость некоторых широко используемых языков программирования.

«Широко используемые языки, такие как C и C++, обеспечивают большую свободу и гибкость в управлении памятью, в то же время в значительной степени полагаясь на программиста для выполнения необходимых проверок ссылок на память».

Если программисту не удастся выполнить надлежащие проверки, эта гибкость может привести к использованию уязвимостей в памяти. Примеры проблем с памятью, которые можно использовать, включают переполнение буфера и сбои в выделении и освобождении памяти. Другие непредвиденные последствия динамического управления памятью включают неправильные результаты программы, снижение производительности, сбои программы и условия гонки.

Хотя разработчики могут попытаться решить проблемы с памятью с помощью внешних инструментов, логические ошибки могут привести к неожиданному поведению программы, например, к доступу к освобожденной памяти. Кроме того, опытные цифровые нарушители могут оторваться от обычного потока выполнения программы, чтобы вызвать проблемы с памятью в своих интересах, например, предоставив специально созданный ввод.

Фаззинг, метод обнаружения проблемных входных данных, продвинулся семимильными шагами благодаря специальным инструментам, доступным в настоящее время на рынке. Этот метод может позволить злоумышленнику получить доступ к определенным участкам памяти, выделить память во время выполнения программы или захватить всю систему.

Список безопасных для памяти языков АНБ

АНБ рекомендует безопасные для памяти языки программирования, такие как C#, Go, Java, Ruby, Rust и Swift.

Однако переход с одного языка программирования на другой является дорогостоящим и длительным процессом и может занять в лучшем случае десятилетия. Кроме того, объем исходного кода C/C++ ошеломляет.

«Смена языков разработки может оказаться непростой задачей. В конце концов, до сих пор существуют приложения, написанные на Коболе. Хотя во многих случаях языки программирования, которые рекомендует АНБ, имеют и другие преимущества, и количество квалифицированных программистов растет», — сказал Майк Паркин, старший технический инженер Vulcan Cyber.

Безопасные для памяти языки, которые могли бы заменить C/C++, такие как Go и Rust, либо имеют крутые кривые обучения, либо меньше пользователей, хотя в последнее время их число увеличилось. Тем не менее, АНБ признает, что безопасный для памяти язык может повысить безопасность за счет «усиленной защиты кода», такой как конфигурации операционной системы и параметры компилятора и инструментов.

По данным АНБ, защита компиляции и времени выполнения, предлагаемая безопасными для памяти языками, может предотвратить большинство проблем.

«С этим руководством АНБ является одним из многих, кто утверждает, что пришло время перейти от C/C++ (и, в некоторых случаях, ассемблера) к другим языкам, которые более безопасны для памяти», — сказал Сэмми Мигес, главный научный сотрудник Synopsys Software. Группа честности. «Различные исследования показали, что небезопасные для памяти языки являются причиной непропорционально большого количества проблем с программным обеспечением».

Тем не менее безопасные для памяти языки не являются панацеей от проблем управления памятью, поскольку программам иногда требуется небезопасный доступ к памяти для выполнения определенных задач.

Некоторые безопасные для памяти языки, такие как C#, также допускают динамическое выделение памяти, когда программисту нужны такие функции. Однако динамическое выделение памяти встречается редко и влияет только на ограниченные части программы, в отличие от поведения по умолчанию в C/C++. Таким образом, внедрение безопасных для памяти языков является наиболее подходящим шагом для устранения уязвимостей, связанных с памятью, которые вызывают множество серьезных ошибок в различных отраслях.

«Поэтому всеобъемлющее сообщество разработчиков программного обеспечения в частном секторе, академических кругах и правительстве США начали инициативы по развитию культуры разработки программного обеспечения в сторону использования безопасных для памяти языков», — пишет АНБ.

Однако Мигес предупреждает, что «рефакторинг миллионов, а может быть, даже триллионов строк кода C/C++, используемых буквально в миллиардах развернутых устройств, на новый язык — неразумная просьба».

Джон Бамбенек, главный охотник за угрозами в Netenrich, предположил, что директива федералов создает ощущение безотлагательности и исходит из «знаний, которые есть у них, а у нас нет».

«Хотя Агентство национальной безопасности (АНБ) имеет заслуженную репутацию секретности и других вещей, оно также известно тем, что дает надежные рекомендации по безопасности, когда на карту поставлены национальные интересы.

Учитывая приведенную здесь рекомендацию, она разумна, хотя на практике ее может быть сложно реализовать», — заключил Паркин». ***(Alicia Hope. NSA Urged Software Developers and Operators to Shift to Memory-Safe Languages // CPO Magazine (https://www.cpomagazine.com/cyber-security/nsa-urged-software-developers-and-operators-to-shift-to-memory-safe-languages/). 18.11.2022).***

***

«Великобритания запустила программу сканирования уязвимостей, которая будет отслеживать все интернет-устройства страны на наличие потенциальных неисправленных проблем, стремясь как укрепить национальную безопасность, так и помочь отдельным организациям защитить себя.

Программа сканирования уязвимостей проводится Национальным центром кибербезопасности (NCSC) и будет проверять все подключенные интернет-устройства в стране на наличие версий программного обеспечения, выявляя устаревшие установки с известными уязвимостями. Правительство заявляет, что оно будет регистрировать только эти версии программного обеспечения вместе с датой, временем и IP-адресом, но если личная информация будет непреднамеренно получена, она будет удалена.

Сканирование уязвимостей по всей стране направлено на создание постоянных «моментальных снимков» кибер-готовности.

Технический директор NSCS Ян Леви сказал, что сканирование уязвимостей очень похоже на то, что часто делают частные охранные фирмы, чтобы заблаговременно обнаруживать потенциальные уязвимости и предупреждать затронутые стороны. В дополнение к предоставлению средств, побуждающих потенциальных жертв исправлять свои интернет-устройства до того, как злоумышленники доберутся до них, программа предоставляет средства сбора данных для таких вещей, как количество времени, которое требуется большинству организаций для исправления серьезной уязвимости. как только это будет раскрыто.

Новая программа сканирования уязвимостей будет связана с существующей службой раннего предупреждения, которая ранее была добровольной программой, но не проводила активного сканирования участников. Теперь все интернет-устройства в стране будут сканироваться, но можно отказаться, направив в агентство по электронной почте список IP-адресов, подлежащих исключению.

Леви также сказал, что сканирование уязвимостей со временем будет становиться все более сложным, и что по мере добавления в процесс новых элементов в интересах прозрачности будут публиковаться дальнейшие публичные разъяснения. Агентство также пообещало регулярные проверки и возможность подавать отчеты о злоупотреблениях. Более подробная информация о будущих разработках была обещана на конференции CYBERUK в Белфасте в апреле 2023 года.

Персональные интернет-устройства будут включены в сканирование

Организации и частные лица должны ожидать сканирования с URL-адреса scan.scanning.service.ncsc.gov.uk и двух IP-адресов (18.171.7.246 и 35.177.10.231). NCSC заявляет, что тестирует свои инструменты и зонды внутри компании, прежде

чем сканировать какие-либо интернет-устройства, и что у нее нет никаких «гнусных» целей. В нем говорится, что запросы предназначены для получения минимально возможного объема информации для целей сканирования уязвимостей. Однако некоторые люди могут видеть оповещения, привязанные к этим адресам, если у них установлено программное обеспечение безопасности.

Сканирование уязвимостей, вероятно, не является чем-то таким, чего уже не делают крупные компании (или заключают контракты с фирмой по обеспечению безопасности). Малые предприятия, у которых нет значительного бюджета на ИТ и у которых нет людей для правильной настройки и защиты интернет-устройств, скорее всего, получат наибольшую выгоду от этой программы, если правительство сможет найти способ сделать свою систему уведомлений эффективной.

Хотя в новостях могут быть некоторые естественные проблемы с конфиденциальностью, сканирование уязвимостей, похоже, ничем не отличается от того, что регулярно делают многочисленные злоумышленники, чтобы найти уязвимые места, где бы они ни находились. Shodan, нейтральный инструмент, который постоянно сканирует Интернет, выполняет по сути ту же функцию и доступен каждому.

Дэвид Мейнор (David Maynor), старший директор по анализу угроз Cybrary, считает это положительным моментом: «Организации, проводящие широкомасштабное интернет-сканирование, теперь стали обычным явлением благодаря таким инструментам, как Masscan. Я думаю, что это положительный признак того, что правительство Великобритании продолжает укреплять свою безопасность».

И Крис Вон (вице-президент по техническому управлению счетами, EME, Tanium) соглашается: «Я ожидаю, что эта инициатива расширит возможности правительства по отчетности на уровне сектора, что поможет свести к минимуму влияние уязвимостей. Это также позволит NCSC сообщать владельцам систем о проблемах безопасности и нести ответственность за своевременное развертывание исправлений. Несмотря на эти преимущества, я знаю, что некоторые люди будут обеспокоены аспектами конфиденциальности этого упражнения, поэтому я думаю, что NCSC был прав, заявив, что сканирование предназначено для сбора минимального количества информации, необходимой для проверки того, затронут ли сканируемый объект уязвимость».

«Я приветствую это развитие и надеюсь, что оно достигнет такого же уровня успеха, как и в других странах, запустивших аналогичные программы, таких как Норвегия. Если он окажется популярным, не удивляйтесь, если сложность начальных сканирований будет постепенно увеличиваться», — добавил Мейнор.

Естественные опасения по поводу деятельности правительства по сканированию

Тем не менее, тот простой факт, что используется слово «сканирование», может привести к тому, что люди, не знакомые с тем, как проводится сканирование уязвимостей (или подавляющее большинство населения), ошибочно полагают, что эта программа предназначена для сканирования интернет-трафика и захвата таких вещей, как личные сообщения или данные о местоположении. Проблема не решается планом, который был предложен несколько месяцев назад и предусматривал

активное сканирование всех британских телефонов и интернет-устройств на стороне клиента на наличие изображений жестокого обращения с детьми, который поддерживался и продвигался NCSC и GCHQ. Для этого потенциально потребовалось бы, чтобы поставщики мобильных ОС или приложений для социальных сетей встроили технологию для активного сканирования устройств, при этом любые помеченные изображения передаются для проверки НПО по защите детей. План был встречен резкой критикой, поскольку, по сути, предполагал взлом сквозного шифрования и все еще находится на рассмотрении правительства. Это был не первый шаг правительства к прекращению сквозного шифрования с использованием жестокого обращения с детьми в качестве мотиватора, поскольку в начале 2022 года он также подвергся резкой критике в связи с рекламной кампанией «Негде спрятаться», проводимой Министерством внутренних дел.

В последнее время NCSC прилагает другие усилия, чтобы помочь британским организациям сканировать уязвимости и защищать свои интернет-устройства, делая доступными через Github сценарии NMAP Scripting Engine, которые помогают пользователям сканировать свою собственную сеть на предмет потенциальных брешей, через которые могут проскользнуть злоумышленники. Это также текущая программа, и NCSC заявляет, что выпустит новые сценарии NMAP для критических уязвимостей безопасности, которые, по ее мнению, будут активно использоваться злоумышленниками». ***(Scott Ikeda. Government Vulnerability Scanning of All UK Internet Devices Begins // CPO Magazine (https://www.cpomagazine.com/cyber-security/government-vulnerability-scanning-of-all-uk-internet-devices-begins/). 15.11.2022).***

***

«Набор из пяти эксплуатируемых уязвимостей в драйвере графического процессора Arm Mali остается неисправленным спустя месяцы после того, как производитель чипов исправил их, в результате чего потенциально миллионы устройств Android могут быть подвержены атакам.

Устройства от Google, Samsung, Xiaomi, Oppo, а также других производителей телефонов в настоящее время затронуты и ждут исправления, которое дойдет до пользователей.

В отчете, опубликованном командой Google Project Zero, подчеркивается «пробел в исправлениях», который мешает цепочке поставок в Android, поскольку обычно требуется несколько месяцев, чтобы обновления безопасности прошивки поступали на затронутые устройства.

Партнерам-производителям оригинального оборудования (OEM) нужно время, чтобы протестировать исправления и внедрить их в свои устройства — процесс, который увеличивает время до достижения устройств конечных пользователей.

Недостатки и влияние

Project Zero обнаружил уязвимости в июне 2022 года. Они отслеживаются как CVE-2022-33917 и CVE-2022-36449 (собирательный идентификатор для нескольких проблем безопасности).

CVE-2022-33917 позволяет непривилегированному пользователю выполнять неправильные операции обработки GPU для получения доступа к свободным разделам памяти. Уязвимость затрагивает драйверы ядра графического процессора Arm Mali от Valhall r29p0 до r38p0.

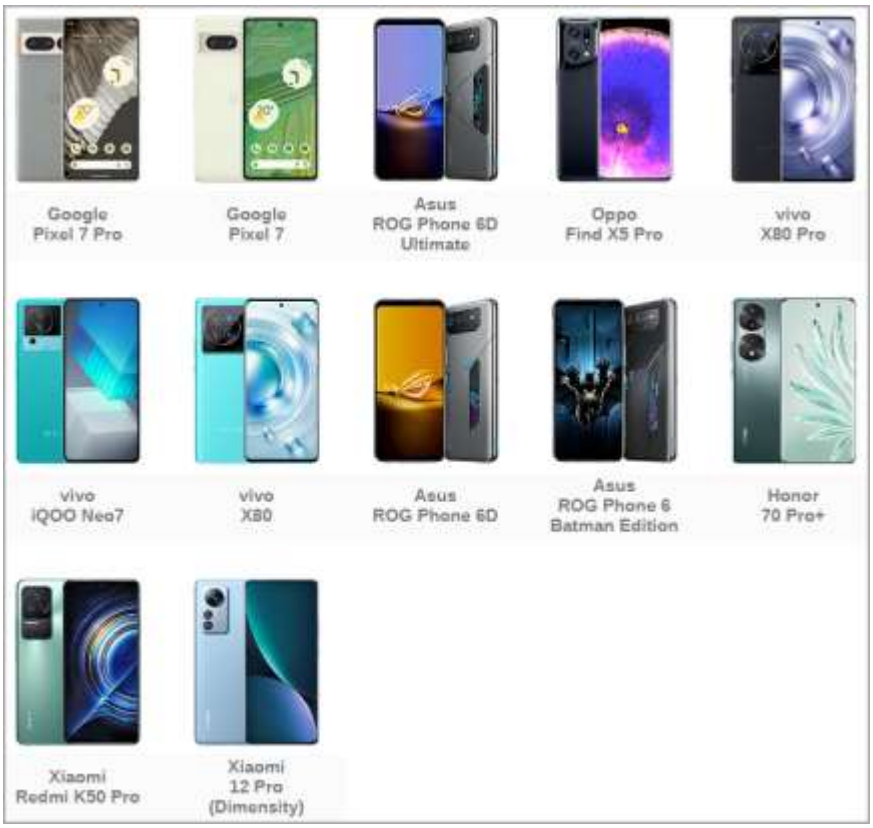
Второй идентификатор, CVE-2022-36449, содержит проблемы, которые позволяют непривилегированному пользователю получать доступ к освобожденной памяти, записывать данные за пределы буфера и раскрывать сведения о сопоставлении памяти.

Это влияет на драйверы ядра графического процессора Arm Mali от Midgard r4p0 до r32p0, Bifrost от r0p0 до r38p0 и r39p0 до r38p1 и Valhall от r19p0 до r38p0 и r39p0 до r38p1.

Project Zero отслеживает эти проблемы как 2325, 2327, 2331, 2333 и 2334 и раскрывает технические детали для каждой из них вместе с демонстрационным кодом.

Несмотря на то, что степень серьезности проблем средняя, их можно использовать и они влияют на большое количество устройств Android.

Драйверы Valhall используются в чипах Mali G710, G610 и G510, установленных в Google Pixel 7, Asus ROG Phone 6, Redmi Note 11 и 12, Honor 70 Pro, RealMe GT, Xiaomi 12 Pro, Oppo Find X5 Pro и Reno 8 Pro., Motorola Edge и OnePlus 10R.



Устройства Android с чипом Mali G710 (GSMArena)

Драйверы Bifrost используются в более старых (2018 г.) чипах Mali G76, G72 и G52, используемых Samsung Galaxy S10, S9, A51 и A71, Redmi Note 10, Huawei P30 и P40 Pro, Honor View 20, Motorola Moto G60S и Realme. 7.

Драйверы Midgard используются в еще более старых (2016 г.) чипах серий Mali T800 и T700, особенно в Samsung Galaxy S7 и Note 7, Sony Xperia X XA1, Huawei Mate 8, Nokia 3.1, LG X и Redmi Note 4.

Пользователи ничего не могут сделать, чтобы смягчить эти недостатки, кроме как ждать, пока поставщик предоставит соответствующие исправления, и следить за потенциальными угрозами.

Крайне маловероятно, что более старые модели, использующие драйверы Midgard, получат исправление исправления, поэтому их следует полностью заменить.

Драйверы графического процессора Mali используются схемами «система на кристалле» от таких поставщиков, как MediaTek, HiSilicon Kirin и Exyno, на которых работает большинство Android-устройств на рынке.

На данный момент исправление от Arm не дошло до OEM-партнеров и тестируется на устройствах Android и Pixel. Через несколько недель Android предоставит исправление своим партнерам, которые несут ответственность за внедрение исправления». ***(Bill Toulas. Mali GPU 'patch gap' leaves Android users vulnerable to attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/mali-gpu-patch-gap-leaves-android-users-vulnerable-to-attacks/). 23.11.2022).***

***

«Компания Acer устранила серьезную уязвимость, затрагивающую несколько моделей ноутбуков, которая могла позволить локальным злоумышленникам деактивировать UEFI Secure Boot на целевых системах.

Функция безопасности безопасной загрузки блокирует ненадежные загрузчики операционных систем на компьютерах с чипом Trusted Platform Module (TPM) и прошивкой Unified Extensible Firmware Interface (UEFI), чтобы предотвратить загрузку вредоносного кода, такого как руткиты и буткиты, во время процесса запуска.

Исследователь вредоносных программ ESET Мартин Смолар сообщил, что уязвимость безопасности (CVE-2022-4020) была обнаружена в драйвере HQSwSmiDxe DXE на некоторых потребительских ноутбуках Acer.

Злоумышленники с высокими привилегиями могут злоупотреблять им в атаках низкой сложности, которые не требуют вмешательства пользователя для изменения параметров безопасной загрузки UEFI путем изменения переменной BootOrderSecureBootDisable NVRAM для отключения безопасной загрузки.

«Исследователи выявили уязвимость, которая может позволить изменить параметры безопасной загрузки путем создания переменных NVRAM (фактическое значение переменной не важно, только наличие проверяется драйверами затронутой прошивки)», — говорится в сообщении Acer.

Воспользовавшись уязвимостью на уязвимых ноутбуках Acer и отключив безопасную загрузку, злоумышленники могут перехватить процесс загрузки ОС и загрузить неподписанные загрузчики для обхода или отключения средств защиты и развертывания вредоносных полезных нагрузок с системными привилегиями.

Полный список затрагиваемых моделей ноутбуков Acer включает Acer Aspire A315-22, A115-21, A315-22G, Extensa EX215-21 и EX215-21G.

Доступно обновление BIOS, ожидается обновление Windows

«Acer рекомендует обновить BIOS до последней версии, чтобы решить эту проблему. Это обновление будет включено как критическое обновление Windows», — добавили в компании.

В качестве альтернативы клиенты могут загрузить обновление BIOS с веб-сайта поддержки компании и установить его вручную на уязвимых системах.

Lenovo исправила аналогичные ошибки, обнаруженные исследователями ESET в нескольких моделях ноутбуков ThinkBook, IdeaPad и Yoga ранее в этом месяце, которые могли позволить злоумышленникам деактивировать UEFI Secure Boot.

Разрешение злоумышленникам запускать неподписанный вредоносный код перед загрузкой ОС может привести к серьезным последствиям, включая развертывание вредоносных программ, которые могут сохраняться между переустановками ОС, и обход средств защиты от вредоносных программ, предоставляемых решениями безопасности.

В случае Lenovo проблема была вызвана тем, что разработчики компании включили драйвер ранней разработки в производственные драйверы, которые могли изменить параметры безопасной загрузки из ОС.

В январе ESET обнаружила еще три уязвимости прошивки UEFI, которые могут позволить злоумышленникам взломать процедуру запуска более чем на 70 моделях устройств Lenovo под управлением Windows». ***(Sergiu Gatlan. Acer fixes UEFI bugs that can be used to disable Secure Boot // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/acer-fixes-uefi-bugs-that-can-be-used-to-disable-secure-boot/). 28.11.2022).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«CISA настоятельно рекомендует всем организациям внедрить MFA, устойчивую к фишингу, для защиты от фишинга и других известных киберугроз.

CISA выпустила два информационных бюллетеня, чтобы выделить угрозы для учетных записей и систем, использующих определенные формы многофакторной аутентификации (MFA). CISA настоятельно рекомендует всем организациям внедрить MFA, устойчивую к фишингу, для защиты от фишинга и других известных киберугроз. Если организация, использующая MFA на основе мобильных push-уведомлений, не может внедрить MFA, устойчивую к фишингу, CISA рекомендует использовать сопоставление номеров, чтобы снизить утомляемость MFA. Хотя сопоставление номеров не так надежно, как MFA, устойчивое к фишингу, оно

является одним из лучших временных мер для организаций, которые не сразу смогут внедрить MFA, устойчивую к фишингу.

CISA рекомендует пользователям и организациям ознакомиться с информационными бюллетенями CISA Реализация защищенной от фишинга MFA и Реализация сопоставления номеров в приложениях MFA. Посетите сайт CISA.gov/MFA для получения дополнительной информации о MFA, включая инфографику иерархии вариантов MFA». ***(CISA Releases Guidance on Phishing-Resistant and Numbers Matching Multifactor Authentication // Homeland Security Today (https://www.hstoday.us/federal-pages/dhs/cisa-releases-guidance-on-phishing-resistant-and-numbers-matching-multifactor-authentication/). 02.11.2022).***

***

«CISA призывает всех людей и организации в сообществе кибербезопасности принять TLP 2.0.

Во вторник CISA официально обновила протокол Traffic Light Protocol (TLP) 2.0, что облегчает более широкий обмен информацией и совместную работу. CISA произвела это обновление в соответствии с рекомендацией Форума групп реагирования на инциденты и безопасности по обновлению до TLP 2.0 к январю 2023 года.

Ключевые обновления TLP 2.0:

TLP 2.0 заменяет TLP:WHITE на TLP:CLEAR.

TLP 2.0 добавляет обозначение TLP:AMBER+STRICT, которое указывает получателю хранить информацию только в пределах своей организации.

Примечание. Функция автоматизированного обмена индикаторами (AIS) CISA не будет обновляться с TLP 1.0 до TLP 2.0 до марта 2023 года. Это исключение включает использование AIS следующих открытых стандартов: Структурированное выражение информации об угрозах (STIX™) для индикаторов киберугроз и защитных мер. информации и Trusted Automated Exchange of Intelligence Information (TAXII™) для связи между машинами.

CISA призывает всех людей и организации в сообществе кибербезопасности принять TLP 2.0. Для получения дополнительной информации см. веб-страницу TLP CISA, www.cisa.gov/tlp, и веб-страницу TLP FIRST, https://www.first.org/tlp/...» ***(CISA Upgrades to TLP 2.0 // Homeland Security Today (https://www.hstoday.us/federal-pages/dhs/cisa-upgrades-to-tlp-2-0/). 02.11.2022).***

***

«Microsoft объявила, что встроенная защита обычно доступна для всех устройств, подключенных к Defender for Endpoint, платформе защиты конечных точек компании.

После применения этот набор параметров по умолчанию обеспечивает лучшую защиту конечных точек предприятия от сложных и новых угроз, включая атаки программ-вымогателей.

«Первоначально встроенная защита будет включать в себя включение защиты от несанкционированного доступа для вашего арендатора, а вскоре появятся и другие настройки по умолчанию», — поясняет Microsoft.

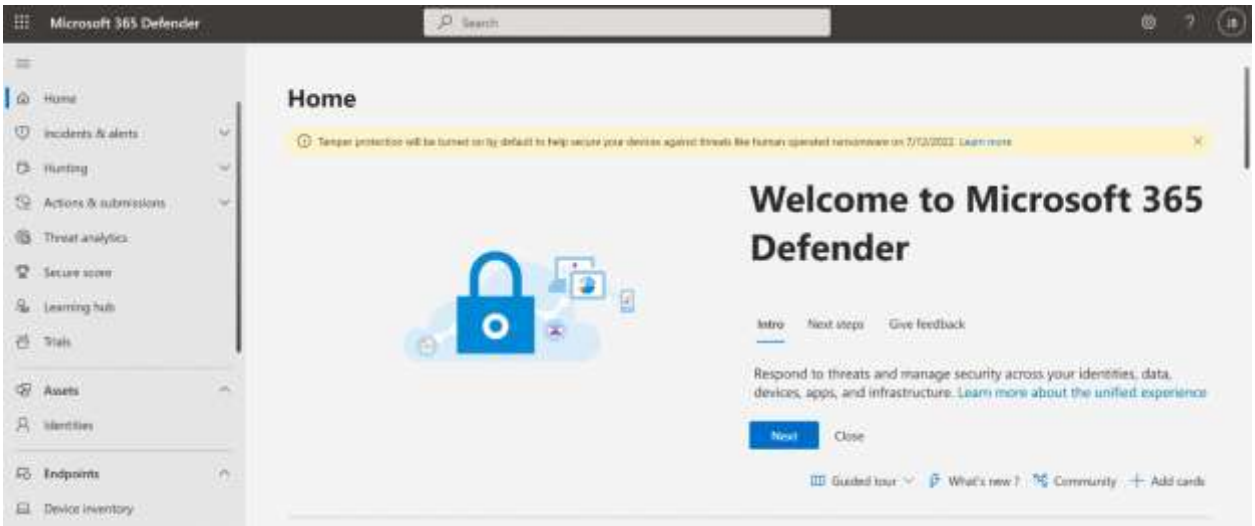
Пока Редмонд не развернет дополнительные параметры защиты по умолчанию с помощью встроенной защиты, администраторы могут включить облачную защиту.

Это объявление было сделано после того, как компания начала включать защиту от несанкционированного доступа для всех новых клиентов с лицензиями Defender for Endpoint Plan 2 или Microsoft 365 E5, начиная с прошлого года.

В сентябре Редмонд добавил, что вскоре он включит защиту от несанкционированного доступа по умолчанию на всех встроенных системах Microsoft Defender для конечной точки (MDE), заблокировав антивирусную программу Microsoft Defender для защиты значений по умолчанию и предотвратив любые изменения параметров безопасности.

«Для дополнительной защиты наших клиентов мы объявляем, что защита от несанкционированного доступа будет включена для всех существующих клиентов, если только она не была явно отключена на портале Защитника Microsoft 365», — сказал Джош Брегман, главный менеджер по продуктам Microsoft, на конференции. время.

Это достигается путем блокировки других приложений от изменения параметров защиты в режиме реального времени и в облаке, мониторинга поведения и компонентов Защитника, таких как IOfficeAntivirus (IOAV), который обрабатывает обнаружение подозрительных файлов, загруженных из Интернета.



Баннер защиты от несанкционированного доступа на портале Microsoft 365 Defender (Майкрософт)

Развертывание для арендатора рядом с вами

Клиенты, которые еще не настроили защиту от несанкционированного доступа в своих корпоративных средах, вскоре получат уведомления на портале Защитника Microsoft 365, предупреждающие их о том, что эта функция будет включена.

«Защита от несанкционированного доступа будет включена для вашего арендатора и будет применяться к устройствам Windows в вашей организации», — сообщает Microsoft на своем портале поддержки.

«Каждый раз, когда новые устройства подключаются к Defender for Endpoint, встроенные параметры защиты будут применяться ко всем новым устройствам под управлением Windows».

Однако администраторы также могут изменить свои встроенные параметры защиты или отказаться от них:

Перейдите на портал Защитника Microsoft 365 и войдите в систему.

Выберите « Настройки » > « Конечные точки » > « Дополнительные функции ».

Установите для параметра Защита от несанкционированного доступа значение Вкл. (если он еще не включен), а затем выберите Сохранить настройки (пока не покидайте эту страницу).

Установите для параметра Защита от несанкционированного доступа значение Выкл., а затем выберите Сохранить настройки.

Администраторы Microsoft 365 также могут исключить некоторые устройства в сети из защиты от несанкционированного доступа, если есть проблемы с совместимостью приложений, используя Управление безопасностью для Defender for Endpoint или создав профиль в Microsoft Endpoint Manager…». ***(Sergiu Gatlan. Microsoft Defender boosts default protection for all enterprise users // Bleeping Computer® (https://www.bleepingcomputer.com/news/microsoft/microsoft-defender-boosts-default-protection-for-all-enterprise-users/). 29.11.2022).***

***

«Незалежна лабораторія AV-Test провела дослідження антивірусних продуктів для Windows 11 та склала відповідний рейтинг.

Вбудований у систему за умовчанням антивірус Microsoft Defender виявився практично «нульовим» і зайняв останнє місце.

Серйозні результати показали такі рішення:

V3 Internet Security 9.0 (AhnLab);

Avast Free AntiVirus 22.6 та 22.7;

Avast One Essential 22.6;

AVG Internet Security 22.6 та 22.7;

Avira Internet Security для Windows 1.1;

Bitdefender Internet Security 26.0;

GData Total Security 25.5;

K7 Security Total Security 16.0;

Kaspersky Internet Security 21.3 Malwarebyte Premium 4.5;

Norton 360 22.22». ***(Вбудований у Windows 11 антивірус Microsoft Defender виявився найгіршим за якістю захисту // Internetua (https://internetua.com/vbudovanii-u-windows-11-antivirus-microsoft-defender-viyavivsya-naigirshim-za-yakistua-zahistu). 20.11.2022).***

***

«У Росії громадяни на пропагандистських телеканалах побачили «оригінальне» привітання до дня ракетних військ та артилерії РФ. Замість звернення диктатора Володимира Путіна можна було побачити привітання від Збройних сил України.

Відео опублікували на сторінці СтратКом ЗСУ у Telegram.

Зокрема, хакери змонтували ролик, де показали росіянам справжні масштаби втрат Росії у війні з Україною. На відео йдеться, що таких втрат історія російської армії ще не бачила.

«Ласкаво просимо до пекла. Не так, не так - Welcome To Ukraine», - говориться на початку відео.

Також росіянам показали, що з початку повномасштабного вторгнення в Україну було ліквідовано понад 83 тисячі російських окупантів.

До того ж перерахували втрати путінської армії у техніці. Російські окупанти втратили 1865 одиниць артилерійських систем, 393 одиниці реактивних систем залпового вогню.

Окрім того, росіянам розповіли, що ЗСУ було героїчно знищено 480 російських крилатих ракет і чотири оперативно-тактичних ракетних комплексів.

«Хакери від імені ЗСУ «привітали» на російському телебачені ракетні війська і артилерію Росії з професійним святом, гарно потролили та показали масштаби їх втрат», - йдеться в повідомленні». ***(«Ласкаво просимо до пекла»: хакери зламали російське ТБ та показали «привітання» від ЗСУ // Internetua (https://internetua.com/-laskavo-prosimo-do-pekla-hakeri-zlamali-rosiiske-tb-ta-pokazali-privitannya-vid-zsu). 19.11.2022).***

***

«Нещодавно компанія RSA представила автентифікатор DS100 – багатофункціональне рішення безпеки, що працює без пароля та може значною мірою покращити взаємодію з користувачем, одночасно знизивши загальну вартість ресурсів. Рішення RSA в Україні просуває офіційний дистриб’ютор ELKO Ukraine.

Як повідомляється, DS100 – це перший автентифікатор, що підтримує хмарний режим та поєднує у собі криптографічні переваги протоколів FIDO з перевагами безпеки одноразового пароля (OTP). На відміну від інших аналогів, DS100 може працювати, як підключеним до мережі, так і відключеним, що робить його гнучким рішенням автентифікації.

Попри те, що DS100 розгортається фізично, ним керують у хмарі за допомогою Cloud Authentication Service. Це дає змогу підвищити ефективність управління без шкоди для безпеки повнофункціонального апаратного автентифікатора.

Незалежно від того, чи використовується логін FIDO2, чи OTP, користувачам не потрібно покладатися на традиційні облікові дані, які важко запам'ятати. Автентифікуватись можна за допомогою біометричного чи іншого методу для FIDO2 або просто натиснувши кнопку, щоб створити код OTP.

Сертифікований FIDO2 DS100 забезпечує безпечний і зручний FIDO2 без пароля автентифікацію у середовищах, де апаратні автентифікатори є бажаними або навіть вимагається для використання. Він легко підключається через роз'єм USB, а також має сучасні функції NFC.

У захищеному середовищі, де USB-з'єднання недоступне, або де користувачу потрібно під'єднатися до VPN, DS100 надає підключену і відключену-OTP функцію входу. Пристрій відображає OTP через екран і за допомогою кнопки OTP реалізує вхід на ресурси автоматично». ***(ELKO Ukraine пропонує апаратний автентифікатор RSA DS100, що спрощуйте керування хмарою // Компьютерное Обозрение (https://ko.com.ua/elko_ukraine_proponuye_aparatnij_avtentifikator_rsa_ds100_shho_sproshhujte_keruvannya_hmaroyu_142683). 23.11.2022).***

***

«Netskope планирует запустить дата-центр в Варшаве в начале 2023 года. Это будет первая инвестиция такого рода в этой части Европы. В то же время компания создала новую должность в Польше в качестве регионального директора, отвечающего за продажи в стране, Центральной и Восточной Европе. На эту должность назначен Михал Боровецкий.

Netskope — американская компания, мировой лидер в области кибербезопасности, которая предоставляет клиентам по всему миру унифицированную платформу безопасности SASE (Secure Access Service Edge). Его задача — защитить данные и пользователей вне зависимости от типа используемого приложения, местоположения и устройства, с которого осуществляется этот доступ.

«Наше исследование показывает, что сотрудники среднего предприятия используют более 2400 облачных приложений. 95 процентов таких решений не управляются ИТ-командами и не контролируются соответствующей организацией. Такие приложения находятся в серой зоне, которую мы относим к «тенью». Эти цифры показывают масштаб явления и проблемы, с которыми сталкиваются компании, работая над защитой своих данных», — сказал Ксавье Дайк, вице-президент Netskope по продажам в Северной и Восточной Европе и регионе DACH». ***(Global leader in cyber security enters Polish market // Warsaw Business Journal (https://wbj.pl/global-leader-in-cyber-security-enters-polish-market/post/136286). 07.11.2022).***

***

«Компания Wipro, предоставляющая технологические услуги и консалтинг, объявила о новой консультационной службе по стратегической кибербезопасности в Европе, призванной предоставить клиентам комплексное решение для борьбы с угрозами безопасности.

Новое предложение, предлагаемое через Wipro CRS Europe, позволит клиентам получить доступ ко всему спектру возможностей компании в области кибербезопасности, от стратегии и внедрения до управляемых услуг.

Тони Буффоманте, старший вице-президент Wipro и глобальный руководитель службы кибербезопасности и управления рисками (CRS), сказал, что предприятия по всей Европе сталкиваются с новыми проблемами из-за эскалации киберугроз — проблема, усугубляемая быстро меняющейся нормативно-правовой средой.

«Наш обширный опыт в области кибербезопасности, глобальная сеть специалистов по кибербезопасности в сочетании с нашими расширенными консультационными возможностями помогут клиентам опережать возникающие угрозы и быстро и гибко адаптироваться к меняющейся нормативно-правовой среде», — сказал он. «Мы очень рады быть представить это предложение клиентам на этом рынке в этот критический момент».

Компания Wipro со штаб-квартирой в Бангалоре, Индия, занимает видное место на мировой арене технологических услуг и консалтинга. В фирме работает более 250 000 сотрудников и деловых партнеров в 66 странах, включая глобальную сеть из более чем 9 000 специалистов по кибербезопасности.

Появление нового предложения по консалтингу в области кибербезопасности последовало за рядом недавних глобальных приобретений в сфере консалтинга: фирма приобрела австралийскую фирму по кибербезопасности Ampion, поставщика консалтинговых услуг в области кибербезопасности из Texaca Edgile, а также глобальную управленческую и техническую консалтинговую компанию Capco.

Лондонская компания Capco присоединилась к более широкому бизнесу в марте 2021 года, расширив присутствие Wipro на берегах Великобритании и сделав ее одним из крупнейших поставщиков комплексных консалтинговых, технологических и трансформационных услуг для банковской отрасли.

Теперь все возможности фирмы в области киберконсалтинга будут находиться под эгидой CyberTransform, которая будет предоставляться клиентам вместе с ее предложением управляемых услуг CyberShield.

CyberTransform — это то, что Wipro называет ориентированным на бизнес, ориентированным на стратегию подходом к трансформации кибербезопасности, разработанным для предоставления «действительно целостного подхода 360», чтобы помочь клиентам управлять киберугрозами и повышать устойчивость.

В своем новом предложении Wipro заявила, что ее европейские консультанты будут работать с клиентами над созданием индивидуальных стратегий и решений для решения уникальных задач рынка.

«Наши недавние приобретения в области кибербезопасности, а также наши недавние стратегические наймы в Европе дали нам возможность переосмыслить то, как мы обслуживаем наших клиентов на этом рынке», — пояснил Джон Херманс, глава Wipro CRS Europe.

«Этот запуск объединит весь наш набор кибервозможностей под единым зонтиком, что позволит нам предоставить клиентам действительно комплексное предложение, основанное на стратегии, но отвечающее каждому аспекту их потребностей в кибербезопасности». ***(Daniel Todd. Wipro launches European cyber security consultancy services // Future US LLC***

(https://www.itpro.com/security/369583/wipro-launches-european-cyber-security-consultancy-services). 23.11.2022).

***

«Кембриджский борец за кибербезопасность Darktrace добился успеха благодаря своей новой технологии PREVENT, которая все чаще используется во всем мире для предотвращения злоумышленников до того, как они нанесут ущерб корпоративным и государственным системам.

За три месяца с момента запуска в августе клиенты во всех основных отраслях промышленности купили PREVENT. Многие из основных клиентов базируются в Соединенных Штатах. Бывший глава ЦРУ назвал эту технологию «перевернувшей правила игры».

В их число входят ProPhase Diagnostics, зарегистрированная на NASDAQ биотехнологическая компания, базирующаяся в США; Sellen Construction, ведущая строительная компания США; Rudin Management, одна из крупнейших частных компаний по недвижимости в Нью-Йорке, и Direct Federal Credit Union, кредитный союз США, насчитывающий десятки тысяч членов.

Среди других новых клиентов PREVENT по всему миру — британский поставщик жилья с более чем 50 000 клиентов, международная производственная и дистрибьюторская компания, работающая в более чем 100 странах, и больница в США, в которой работает более 700 сотрудников. Darktrace говорит, что есть много других.

Новые данные, предоставленные Darktrace, показывают, что почти две трети организаций не очень уверены в выявлении своих самых серьезных уязвимостей, а 81% считают, что технология ИИ поможет им автоматизировать свою систему безопасности.

Исследование, связанное с заинтересованностью крупных клиентов, как нельзя более своевременно, поскольку глобальные экономические потери из-за киберпреступлений в год оцениваются в 6 трлн долларов и, по прогнозам, вырастут до 10,5 трлн долларов к 2025 году.

Генеральный директор Darktrace Поппи Густафссон говорит: «Потенциал PREVENT очевиден, поскольку мы видим его отражение в самом длинном списке клиентов, подписавшихся на любой продукт, запущенный в истории Darktrace.

«Эта технология значительно усложняет работу злоумышленника, поскольку она вооружает службы безопасности беспрецедентными инструментами на базе искусственного интеллекта, которые могут предотвратить даже самые сложные кибератаки.

«Это представляет собой фундаментальный сдвиг в кибербезопасности, выдвигающий группы безопасности на передний план, поскольку они стремятся защитить свои организации и повысить устойчивость к киберугрозам».

Эмбер Радд, бывший министр внутренних дел Великобритании и член консультативного совета Darktrace, добавляет: «Угрозы кибербезопасности являются одними из самых серьезных, но наименее понятных рисков, с которыми сегодня сталкиваются организации.

«Поскольку геополитический ландшафт становится все более изменчивым, а мир продолжает двигаться по пути быстрой цифровой трансформации, предприятия сталкиваются с более широким и сложным набором проблем кибербезопасности, чем когда-либо прежде, и они постоянно развиваются.

«Прогнозируемые глобальные экономические потери в результате сбоев в киберпространстве значительны. Проактивность требует от организаций понимания своих слабых сторон и их упреждающего устранения до того, как злоумышленники воспользуются преимуществом.

«Приятно видеть, как Darktrace PREVENT может помочь организациям повысить свою киберустойчивость перед лицом этого меняющегося ландшафта и на фоне глобальной экономической неопределенности».

Бывший крупный игрок ЦРУ Алан Уэйд сказал, что «нет никаких сомнений в том, что следующий этап инноваций в области кибербезопасности должен улучшить способность прогнозировать и предотвращать угрозы со стороны высокоорганизованных и все более изощренных киберпреступников».

Он добавил: «Необходимость в этой возможности ощущается еще острее во время эскалации геополитического конфликта и дефицита квалифицированных кибертехнологов.

«Спрос на Darktrace PREVENT явно отражает более решительную направленность директоров по информационной безопасности на решения, которые позволяют им быть активными и принимать меры до того, как их системы будут взломаны. Это меняет правила игры». ***(Tony Quested. New Darktrace cyber security technology gains traction as ex-CIA man says it's a game-changer // Business Weekly (https://www.businessweekly.co.uk/news/hi-tech/new-darktrace-cyber-security-technology-gains-traction-ex-cia-man-says-it%E2%80%99s-game). 14.11.2022).***

***

«Dell Technologies расширяет свое отраслевое лидерство в области защиты данных, чтобы помочь клиентам защитить свои данные локально, в общедоступных облаках и на периферии.

Устройство Dell PowerProtect Data Manager представляет собой ряд усовершенствований для защиты данных в мультиоблачных средах, которые просты в использовании и просты в использовании. Инновации Dell в области отказоустойчивости и операционной безопасности на основе ИИ ускоряют внедрение архитектур Zero Trust, помогая защитить организации от растущей угрозы кибератак.

Новые решения помогают решить растущие проблемы защиты данных, с которыми сталкиваются организации.

Dell продолжает внедрять инновации в свое программное обеспечение для защиты данных Dell PowerProtect Data Manager, помогающее организациям упростить свои ИТ-операции и снизить риски. Программное обеспечение PowerProtect Data Manager удовлетворяет растущую потребность в киберустойчивости и поддерживает принципы нулевого доверия с новыми встроенными возможностями операционной безопасности, такими как

многофакторная проверка подлинности, двойная авторизация и управление доступом на основе ролей.

Устройство Dell PowerProtect Data Manager Appliance предлагает простой способ внедрения современной защиты данных.

Устройство предлагает покупателям:

- Современная программно-определяемая архитектура: позволяет автоматически обнаруживать и защищать активы, а также обеспечивает уникальную защиту VMware, гарантирующую доступность всех виртуальных машин без нарушения работы бизнеса.
- Безопасное, киберустойчивое решение: обеспечивает более безопасный доступ к ограниченным функциям с помощью управления идентификацией и доступом для повышения киберустойчивости.
- Простой, унифицированный пользовательский интерфейс: обеспечивает программно-определяемую защиту данных, упрощающую развертывание и использование.

Dell расширяет кибервосстановление для быстрых и простых в развертывании общедоступных облачных хранилищ

PowerProtect Cyber Recovery для Google Cloud позволяет клиентам развернуть изолированное киберхранилище в Google Cloud для более безопасного разделения и защиты данных от кибератак. В отличие от стандартных облачных решений для резервного копирования, доступ к интерфейсам управления заблокирован сетевыми элементами управления, и для доступа могут потребоваться отдельные учетные данные безопасности и многофакторная проверка подлинности.

Организации могут использовать свою существующую подписку на Google Cloud для приобретения PowerProtect Cyber Recovery через Google Cloud Marketplace, и эту услугу можно приобрести непосредственно у Dell и ее торговых партнеров.

Новое предложение знаменует собой последнее расширение возможностей Dell по кибервосстановлению для публичных облаков после введения в этом году Dell PowerProtect для Microsoft Azure и CyberSense для Dell PowerProtect Cyber Recovery для AWS.

Dell APEX упрощает хранение резервных копий благодаря гибким вариантам использования

Услуги Dell APEX Data Storage Services расширяются, чтобы предложить опцию Backup Target, чтобы обеспечить более безопасное хранилище резервных копий с оплатой по мере использования и гибкой моделью потребления. Услуга Backup Target проста в использовании и упрощает процесс приобретения, развертывания и обслуживания хранилища резервных копий. Опираясь на передовые решения Dell в области устройств обработки данных и защиты данных1, решение Backup Target помогает сократить объем хранилища, занимаемый заказчиком, и повысить доступность данных». ***(Ray Sharma. Dell Strengthens Cyber Resiliency with Multicloud Data Protection & Security Innovations // THE FAST MODE (https://www.thefastmode.com/technology-solutions/29099-dell-strengthens-cyber-resiliency-with-multicloud-data-protection-security-innovations). 24.11.2022).***

***

«Государственная компания по производству электроэнергии Турции (EÜAŞ) ввела в эксплуатацию собственное программное обеспечение для кибербезопасности на электростанциях.

Генеральный директор EÜAŞ Иззет Алагёз сказал, что программное обеспечение, предназначенное для управления электростанциями, разработанное EÜAŞ под названием «Системы автоматизации EÜAŞ», представляет собой цифровую платформу управления.

«Мы доказали компетентность платформы, используя ее на наших собственных электростанциях», — добавил он.

«Сейчас мы отрабатываем систему на 17-й электростанции. Вместо того, чтобы покупать систему защиты от кибератак, мы разработали систему управления, в которой все коды, железо, софт и все остальное принадлежит нам».

Алагез заявил, что они разработали систему, которая может останавливать кибератаки, добавив, что Турция была одной из пяти стран, которые смогли это сделать.

«Системы автоматизации EÜAŞ, где мы используем самый быстрый в мире микропроцессор и можем проводить самый быстрый анализ отказов, — это система управления, которая есть только в четырех странах мира, и мы стали пятыми после США, Германии, Швейцарии и Японии». Об этом Алагез заявил группе журналистов на 12-м Энергетическом саммите Турции.

Он отметил, что разработка собственной системы защиты от кибератак гарантировала Турции, что у нее не будет черного хода.

«Купленные системы обеспечивают защиту от кибератак, но не защиту от сборщиков систем», — сказал Алагез.

«Вы не можете защитить систему от человека, который ее установил, у него есть ключи. Чтобы эксплуатировать систему без бэкдоров, мы должны установить ее сами. В этом аспекте EÜAŞ Automation System является самой надежной системой управления в Турции. Это мы разработали и установили его, у него нет лазеек». ***(Neşe Karanfil. Türkiye develops own system for cyber security of power plants // Hürriyet Daily News (https://www.hurriyetdailynews.com/turkiye-develops-own-system-for-cyber-security-of-power-plants-178759). 24.11.2022).***

***

«Государственный научно-исследовательский институт Швеции RISE запускает самую передовую в Европе инициативу по кибербезопасности, посвященную испытаниям транспортных средств. RISE Cyber Test Lab for Automotive позволяет автомобильной промышленности тестировать автомобили, используя новейшие кибертехнологии и самые строгие в мире методы испытаний.

Cyber Test Lab предложит ряд беспрецедентных идей, методов и испытательных стендов в сотрудничестве с ведущими мировыми экспертами в области телекоммуникаций и этическими хакерами. Партнерство уникально тем, что решает то, что стало ключевой проблемой для производителей, конкурирующих за создание подключенных автомобилей.

«Мы развертываем ведущий в мире центр с несколькими испытательными стендами и учеными вместе с тщательно отобранными партнерами. Мы будем бороться с растущими киберугрозами вокруг подключенных автомобилей сегодня и в будущем. Один производитель автомобилей не может работать в одиночку в поиске способов борьбы с кибератаками. Это должно быть сделано с использованием самого широкого спектра знаний, чтобы вся отрасль могла извлечь выгоду из централизованных исследований». Саид Пиа Сандвик, генеральный директор RISE

Cyber Test Lab запускается в беспрецедентное для отрасли время. Ключевые данные:

К 2026 г. на автомобили со встроенным подключением будет приходиться около 80% продаж автомобилей с подключением к Интернету (Businesswire, январь 2022 г.).

По данным McKinsey & Company, к 2030 году около 95% новых автомобилей, продаваемых по всему миру, будут подключены к сети, по сравнению с примерно 50% сегодня.

Прогнозируется, что к 2024 году автомобильная промышленность потеряет ошеломляющие 505 миллиардов долларов из-за кибератак. Хакеры становятся все более изощренными: 84,5% атак 2021 года осуществляются удаленно. (Безопасность восходящего потока, январь 2022 г.).

RISE начала планировать создание специальной лаборатории по тестированию автомобильной кибербезопасности в 2021 году после нескольких громких кибератак на автомобили по всему миру. Лаборатория Cyber Test Lab будет тестировать уязвимости в ключевых областях — виртуальное тестирование/цифровые двойники, встроенное программное обеспечение в автомобильных блоках (ECU), облачное программное обеспечение транспортных средств.

Cyber Test Lab предоставляет услуги по тестированию, включая моделирование/виртуализацию, тестирование подсистем, полувиртуальное и полное тестирование транспортных средств в контролируемых средах. Он обеспечивает полную цепочку возможностей тестирования, соединяя наш существующий Cyber Range с автомобильными испытательными стендами AWITAR и Asta Zero. Это позволяет производителям проводить стресс-тестирование новых технологий и продуктов на протяжении всего процесса НИОКР.

«Это может показаться спорным, но мы твердо верим, что работа с этичными хакерами имеет решающее значение для тестирования автомобилей на пределе их возможностей. Этичные хакеры являются выбранными партнерами из нашего существующего Cyber Range в Стокгольме. Этот запуск Cyber Test Lab особенно важен в то время, когда кибератаки и киберугрозы в отношении инфраструктуры и подключенных технологий стали быстрорастущей проблемой во всем мире». — сказал Томас Бодеклинт, руководитель отдела Cyber Test Lab.

Фокус на автомобильной промышленности был очевидной отправной точкой в стране, где находятся одни из самых известных мировых автомобильных компаний, таких как Scania, Volvo Trucks, Volvo Cars и Koenigsegg. Швеция также является домом для новых инновационных стартапов, таких как Einride, Polestar и

Volta Trucks, а также компаний, поставляющих передовые технологии для подключенных и беспилотных транспортных средств.

Организация Европейского Союза по кибербезопасности ENISA уже готовит стандарты и сертификаты ЕС в области кибербезопасности. С запуском Cyber Test Lab компания RISE должна стать ведущим европейским поставщиком методов тестирования и исследований, лежащих в основе этого процесса сертификации.

RISE уже проводит ведущие в мире полигоны для испытаний дорожных систем и исследований беспилотных транспортных средств в AstaZero и AWITAR за пределами Гётеборга. Оба этих испытательных полигона включены в лабораторию Cyber Test Lab.

Лаборатория RISE Cyber Test Lab приступит к расширенному тестированию к началу 2023 года. В процессе подготовки уже полным ходом идут пилотные проекты, имитирующие кибератаки на транспортные средства и инфраструктуру зарядки электромобилей». ***(Sweden launches Europe's most advanced hub for automotive cyber security // Automotive World Ltd (https://www.automotiveworld.com/news-releases/sweden-launches-europes-most-advanced-hub-for-automotive-cyber-security/). 24.11.2022).***

***