**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

№ 4 (квітень)

Київ – 2021

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., 2021.– №4 (квітень) . – 256 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.

ЗМІСТ

«Оператор зв'язку «Київстар» розширює портфель продуктів для бізнес-клієнтів новим актуальним сервісом AntiDDoS – багаторівневим захистом від спрямованого шкідливого трафіку, ефективність якого перевірено на власних IT-системах та мережі оператора. В основі сервісу – рішення FortiDDoS від розробника Fortinet.

Сервіс AntiDDoS працює в інтернет-мережі «Київстар». Він відстежує структуру трафіку, що надходить з інтернету в підмережі (ресурси) клієнта. Щойно система виявляє відхилення від легітимного трафіку, він автоматично переспрямовується на очищення і тільки після цього потрапляє до клієнта.

Серед основних переваг AntiDDoS наводяться:

Система працює в автоматичному режимі без необхідності втручання оператора – незалежно від типу і масштабу атаки;

Робота з трафіком базується не лише на сигнатурному аналізі, а й з використанням машинного навчання, що дозволяє захищати системи як від відомих так і невідомих атак нового типу;

Високоефективне апаратне рішення. Повна перевірка пакетів: двонаправлене виявлення, протидія атакам DDoS рівнів 3, 4 та 7, в т.ч. «об'ємним», атакам SSL Renegotiation/HTTP;

Вичерпна перевірка всього DNS-трафіку для захисту від широкого спектра об'ємних, застосункових та аномальних атак на основі DNS;

Вбудовані засоби комплексної звітності;

Зручне розгортання, налаштування та використання.

Підключити AntiDDoS можна до наявного каналу інтернет від «Київстар». Упродовж 14-30 днів після підключення сервіс «вивчатиме» трафік клієнта, щоб у подальшому використовувати отримані дані для постійного моніторингу.

«У наш час захист від кіберзагроз – це невід’ємна складова розбудови бізнес-процесів компанії. Адже можна скільки завгодно приділяти час стратегії розвитку бізнесу, впроваджувати нові методи заради збільшення прибутків, але в одну мить втратити все через блокування робочих ресурсів зловмисниками», – прокоментував Костянтин Вечір, директор з розвитку бізнесу на корпоративному ринку «Київстар». ***(«Київстар» пропонує бізнес-клієнтам захист від DDoS-атак на базі рішення Fortinet // Компьютерное Обозрение (https://ko.com.ua/kiyivstar_proponuye_biznes-kliyentam_zahist_vid_ddos-atak_na_bazi_rishennya_fortinet_137094). 19.04.2021).***

***

Національна система кібербезпеки

«В Украине в соответствии со ст. 10 Закона Украины «Об основных принципах обеспечения кибербезопасности в Украине", Меморандума, заключенного 14 декабря 2020 года между Аппаратом Совета национальной

безопасности и обороны Украины, Министерством цифровой трансформации Украины и Администрацией Государственной службы специальной связи и защиты информации Украины, создан "независимый коллегиальный совещательный орган, включающий представителей частного и государственного сектора" - Совет информационной и кибербезопасности.

Конечно, в условиях продолжающейся войны СИКБ должен стать действенным органом по предотвращению информационных и кибератак. IT эксперты иронизируют в соцсетях о составе данного органа, где практически нет высококлассных специалистов по кибербезопасности, да и по информационной тоже. У этой структуры имеется и свой сайт с видео мутной воды.

Совет должен решать следующие вопросы:

вовлечение в процесс развития национальной системы кибербезопасности широкого круга субъектов обеспечения кибербезопасности публичного и частного секторов;

усиление роли частного сектора в процессе формирования и реализации публичной политики по развитию сферы кибербезопасности;

внедрение и реализация принципов государственно-частного партнерства в сфере кибербезопасности;

развитие доверия между субъектами национальной системы кибербезопасности;

совершенствование уровня обоснованности государственных управленческих решений в сфере кибербезопасности;

осуществление экспертизы проектов концепций, стратегий, программ, законодательных актов в сфере информационной безопасности и кибербезопасности;

осуществление мониторинга и анализа состояния развития, оценка эффективности и результативности публичной политики информационной безопасности и кибербезопасности.

Состав Совета информационной и кибербезопасности был сформирован на конкурсной основе из числа лиц, подавших свои кандидатуры в состав Совета. Члены Совета избираются на срок сроком два года. Член Совета может быть ее членом не более двух сроков подряд.

Вот только непонятно, чем является данный Совет - расширенным СНБО? Там много управленцев и мало ИТ-шников…». ***(Герман Богапов. В Украине создан Совет информационной и кибербезопасности // InternetUA (http://internetua.com/v-ukraine-sozdan-sovet-informacionnoi-i-kiberbezopasnosti). 07.04.2021).***

***

«Президент України Володимир Зеленський анонсував відкриття "впродовж найближчого місяця" Центру кібербезпеки в рамках протидії дезінформації.

Про це він сповістив в інтерв’ю французькому виданню Le Figaro, яке оприлюднила пресслужба Офісу президента.

Глава держави зазначив, що на запровадження реформ в Україні впливає російська пропаганда та дезінформація, а також війна, на яку витрачаються значні кошти.

У зв'язку з цим він нагадав про появу в Україні Центру протидії дезінформації та анонсував відкриття Центру кібербезпеки.

"Дезінформація, пропаганда. Це у нас одна зі складних ситуацій. В Україні з'явився Центр протидії дезінформації, йому два тижні. Також я збираюся впродовж найближчого місяця офіційно відкрити наш Центр кібербезпеки. Це дуже важливо, щоб протидіяти дезінформації. Дезінформація сьогодні вбиває все – впливає на курс валют, на інвестклімат – ми розуміємо, як перетягують інвесторів, і через це можуть не відкриватися нові фабрики, заводи, значить, не будуть з'являтися нові робочі місця. Тобто проникнення – це такий новий вид конкуренції. На жаль, це нечесна конкуренція. Але це – сучасні виклики, у яких ми живемо. Ми розуміємо, що війна – це таке "теля", яке не можна нагодувати; їй постійно треба давати їжу, гроші, і вона висмоктує з економіки України все", – розповів Зеленський.

Він додав, що в Україні через дії РФ постійно повинні бути напоготові 200-250 тисяч осіб, які "живуть війною".

Коментуючи проблему російських шпигунів, Зеленський заявив, що "кейси є", і в них розбирається СБУ.

"Так. У нас є кейси, знаходимо їх. І розбирається СБУ. Вони можуть бути на різних підприємствах і в деяких державних вертикалях, які керують тим чи іншим напрямом, наприклад енергетичним, середні й малі рівні. СБУ знайшла навіть у себе. Ми не зупиняємось і знаходимо нові випадки", – запевнив Зеленський». ***(Зеленський анонсував відкриття «впродовж місяця» Центру кібербезпеки для протидії дезінформації // Букви (https://bykvu.com/ru/bukvy/zelenskij-anonsuvav-vidkrittja-vprodovzh-misjacja-centru-kiberbezpeki-dlja-protidii-dezinformacii/). 16.04.2021).***

***

«Нацбанк відповідно до закону про кібербезпеку уперше визначив перелік об'єктів критичної інфраструктури у банківській системі України.

Як повідомляє прес-служба регулятора, НБУ відповідно до положень закону «Про основні засади забезпечення кібербезпеки України» назвав банки, стале функціонування яких забезпечує стабільність банківської системи, має суттєве значення для економіки та безпеки держави, функціонування суспільства, та які становлять значний суспільний інтерес. У список критично важливих потрапили банки з переліку системно важливих, і ті, у яких держава прямо чи опосередковано володіє часткою понад 75% від статутного капіталу.

В цілому список об'єктів критичної інфраструктури в банківській системі України виглядає наступним чином:

Національний банк України;

АБ УКРГАЗБАНК;

Акціонерний банк «Південний»;

АТ КБ «ПриватБанк»;

АТ А-БАНК;
АТ АЛЬФА-БАНК;
АТ ОТП БАНК;
АТ «Ощадбанк»;
АТ ПУМБ;
АТ «Райффайзен Банк Аваль»;
АТ ТАСКОМБАНК;
АТ «Укрексімбанк»;
АТ УКРСИББАНК;
АТ УНІВЕРСАЛ БАНК.

Раніше Нацбанк запустив сторінку з основними параметрами 13 системно важливих банків – діяльність таких фінустанов впливає на стабільність усієї банківської системи». ***(НБУ оприлюднив перелік об'єктів критичної інфраструктури у банківській системі // UA.NEWS (https://ua.news/ua/nbu-obnarodoval-perechen-obektov-krytycheskoj-ynfrastruktury-v-bankovskoj-systeme/). 23.04.2021).***

***

Правове забезпечення кібербезпеки в Україні

«Администрация Государственной службы специальной связи и защиты информации Украины обнародовала проект постановления Кабинета Министров Украины «Об утверждении Порядка предоставления услуг Национального центра резервирования государственных информационных ресурсов».

При этом предлагается всем заинтересованным подать свои замечания и предложения в ГСССЗИ до 1 мая 2021 года.

В сообщении службы говорится:

“Проект постановления Кабинета Министров Украины «Об утверждении Порядка предоставления услуг Национального центра бронирования государственных информационных ресурсов» (далее - проект акта) разработан Администрацией Госспецсвязи во исполнение абзаца третьего пункта 5 постановления Кабинета Министров Украины № 94 «О реализации экспериментального проекта по функционированию Национального центра резервирования государственных информационных ресурсов» с целью установления четкой процедуры предоставления услуг Национального центра, определение перечня услуг, которые им будут предоставляться”.

Данное постановление Кабмина датируется 8 февраля и предусматривает:

"Ввести с 1 ноября 2021 функционирования Национального центра резервирования государственных информационных ресурсов.

Администрации Государственной службы специальной связи и защиты информации:

утвердить в месячный срок перечень объектов Национального центра резервирования государственных информационных ресурсов;

подать в трехмесячный срок на утверждение Кабинета Министров Украины порядок предоставления услуг Национального центра резервирования государственных информационных ресурсов;

подать до 31 декабря 2022 Кабинету Министров Украины и Аппарату Совета национальной безопасности и обороны Украины отчет о реализации экспериментального проекта по функционированию Национального центра резервирования государственных информационных ресурсов, а также предложения о внесении изменений в акты законодательства по результатам его реализации".

Кабмин также утвердил “Порядок функционирования Национального центра резервирования государственных информационных ресурсов”, в котором говорится, что Национальный центром “является организованная совокупность объектов, созданных с целью обеспечения надежности и бесперебойности работы государственных информационных ресурсов, киберзащиты, хранения государственных электронных информационных ресурсов, резервного копирования информации и сведений государственных электронных информационных ресурсов государственных органов, воинских формирований (кроме Вооруженных Сил и Главного управления разведки Минобороны), образованных в соответствии с законами, предприятий, учреждений и организаций”.

В структуру НЦРГИР должны входить четыре дата-центра, как минимум два из которых по логике вещей должны быть территориально разнесены:

единые основной и резервный защищенные центры обработки данных, предназначенные для обработки государственных электронных информационных ресурсов

единые основной и резервный защищены центры обработки данных, предназначенные для сохранения государственных электронных информационных ресурсов.

Основными задачами Национального центра являются:

"1) обеспечение непрерывности работы государственных информационных ресурсов, резервного копирования информации и сведений государственных электронных информационных ресурсов государственных органов, воинских формирований (кроме Вооруженных Сил и Главного управления разведки Минобороны), образованных в соответствии с законами, предприятий, учреждений и организаций;

2) обеспечение надежного функционирования серверного оборудования, системы хранения данных, активного сетевого оборудования, архитектурно-технических решений по резервированию и дублированию информационных систем, постоянно работающей инженерной инфраструктуры; осуществления обязательного контроля по статистическим данным работы по физической защите объектов, системы управления и мониторинга информационных систем, комплекса организационных мероприятий;

3) обеспечение преимущества в уменьшении времени доступа к информации, увеличении доступного для каждого пользователя ресурса для хранения данных, увеличении доступности данных для пользователей, отсутствия затрат времени на резервное копирование и восстановление данных, повышении защищенности системы от сбоев в работе и предотвращения потери информации.» ***(Герман***

Богапов. Кабмин создаст Национальный центр резервирования информационных ресурсов // InternetUA (http://internetua.com/kabmin-sozdast-nacionalnyi-centr-rezervirovaniya-informacionnyh-resursov). 09.04.2021).

***

Кібервійна проти України

«Команда реагування на комп'ютерні надзвичайні події України (CERT-UA) виявила факти масових розсилань шкідливого програмного забезпечення, замаскованого під сповіщення "Нової пошти".

Про це проінформували на сторінці підрозділу Держспецзв'язку CERT-UA.

Зазначається, що масові розсилання листів зі вкладеним шкідливим ПЗ (або посиланнями на його завантаження) відбуваються на електронні поштові адреси державних органів України. Зловмисники маскують повідомлення під сповіщення від поштового оператора "Нова пошта".

"Листи містять інформацію начебто від "Нової пошти" щодо надсилання вантажу, вони спонукають перейти за посиланням для перегляду деталей надсилання. За посиланням міститься архів з вмістом шкідливго програмного забезпечення Agent Tesla", — зазначили в команді реагування.

На прикладі, наданому командою, примітно те, що ім'я користувача, від якого надійшов лист — "Нова Пошта", але поштова адреса — з сайту іспанського виробника конвеєрів.

В CERT-UA пояснили, що поширене у такий спосіб шкідливе ПЗ Agent Tesla виконує функції викрадача інформації та є вдосконаленим трояном віддаленого доступу.

Agent Tesla здатне відслідковувати та збирати дані вводу з клавіатури, робити скріншоти та отримувати облікові дані, що використовуються в різних програмах системи.

З'явився Agent Tesla у 2014 році та виконував функції викрадача паролів. Це ПЗ є комерційним, його можна придбати на сайті розробників. І хоча ті закликають використовувати Agent Tesla, не порушуючи закон, цієї поради, вочевидь, зловмисники не дослухаються…» ***(Під виглядом «Нової пошти»: зловмисники пересилають держорганам України небезпечний вірус // Букви (https://bykvu.com/ru/bukvy/pid-vigljadom-novoi-poshti-zlovmisniki-peresilajut-derzhorganam-ukraini-nebezpechnij-virus/). 16.04.2021).***

***

«Ситуаційний центр кібербезпеки СБУ фіксує зростання кількості кібератак, спрямованих на органи державної влади, об'єкти критичної інфраструктури та організації приватного сектору України. Активізувалися переважно хакерські угруповання, підпорядковані спецслужбам РФ, повідомляє прессслужба СБУ.

СБУ постійно вживає заходи із пошуку, виявлення та локалізації зазначених кібератак та кіберінцидентів, а також протидіє кіберзагрозам в ІТС (інформаційно-

телекомунікаційні системи). Крім того, кіберфахівці Служби налагодили взаємодію за допомогою системи обміну даними про кібератаки на базі платформи MISP-UA та інших програмно-апаратних рішень.

В службі закликають українців бути пильними і про всі факти можливих кібератак їм повідомляти:

incident@dis.gov.ua – для повідомлень об’єктів критичної інфраструктури та органів державної влади про виявлені кіберінциденти;

cvd@dis.gov.ua – для повідомлень щодо виявлених вразливостей в інформаційно-телекомунікаційних системах об’єктів критичної інфраструктури та органів державної влади (на умовах Публічного меморандуму);

misp.gov.ua – платформа обміну індикаторами компрометації між об’єктами критичної інфраструктури та органами державної влади, користувачі яких заздалегідь підключені (за умови укладання окремого Меморандуму).

Разом з тим, СБУ починає активне інформування громадськості, у тому числі через публікування звітів щодо конкретних кібератак та індикаторів компрометації. Цю інформацію можна використовувати для організації захисту комп’ютерних мереж і системної протидії кіберзагрозам національній безпеці держави. Також отримані дані дозволять підвищити рівень обізнаності технічних спеціалістів органів державної влади.

Так, у квітні 2021 року виявлено кібератаку на ІТС органів державної влади, з використанням документів-приманок тематики COVID-19. Завантаження зазначених файлів з мережі Інтернет (через поштові повідомлення, групи в месенджерах, тощо) та взаємодія з ними призводила до ураження комп'ютерів користувачів і вивантаження робочих файлів (із заздалегідь заданими розширеннями) на сервери зловмисників…» ***(СБУ фіксує зростання кількості кібератак, спрямованих на органи державної влади, об'єкти інфраструктури та приватні фірми // Дзеркало тижня. Україна (https://zn.ua/ukr/UKRAINE/sbu-fiksuje-zrostannja-kilkosti-kiberatak-sprjamovanikh-na-orhani-derzhavnoji-vladi-objekti-infrastrukturi-ta-privatni-firmi.html). 26.04.2021).***

***

«Фахівці Служби безпеки України не дали спецслужб Російської Федерації здійснити вірусну атаку на держоргани України.

Про це повідомляє пресцентр СБУ на відомчому сайті.

За даними спецслужби, російські куратори діяли через завербованого українського хакера, який повинен був передати українським чиновникам замаскований файл зі шпигунським програмним забезпеченням. Метою атаки були обрані центральні органи влади та органи місцевого самоврядування.

Зловмисник збирався заблокувати роботу об'єктів інформаційної та критичної інфраструктури.

Оперативники встановили, що спецслужби РФ діяли через жителя Запоріжжя. Через інтернет він отримав від громадянина РФ пропозицію конфіденційного співробітництва.

За задумом "кураторів", розсилка повинна була забезпечити вірусне ураження закритих електронних інформаційних систем державних установ і органів місцевого самоврядування.

В ході проведених слідчих дій правоохоронці вилучили електронні носії інформації з файлами наданого іноземними спецслужбами програмного забезпечення, а також листування з кураторами РФ.

Організатору повідомлено про підозру у державній зраді.

Раніше повідомлялося, що ситуаційний центр кібербезпеки СБУ фіксує зростання кількості кібератак, спрямованих на органи державної влади, об'єкти критичної інфраструктури і організації приватного сектора України. Активізувалися переважно хакерські угрупування, підлеглі спецслужбам РФ, повідомляє пресслужба СБУ.

Кіберспеціалісти Служби налагодили взаємодію з допомогою системи обміну даними про кібератаки на базі платформи MISP-UA та інших програмно-апаратних рішень.

У службі закликали українців бути пильними і про всі факти можливих кібератак повідомляти їм:

incident@dis.gov.ua - для повідомлень об'єктів критичної інфраструктури і органів державної влади про виявлені кіберінциденти;

cvd@dis.gov.ua - для повідомлень про виявлені вразливості в інформаційно-телекомунікаційних системах об'єктів критичної інфраструктури та органів державної влади (на умовах Публічного меморандуму);

misp.gov.ua - платформа обміну індикаторами компрометації між об'єктами критичної інфраструктури та органами державної влади, користувачі яких заздалегідь підключені (за умови укладення окремого Меморандуму).

СБУ починає активне інформування громадськості, в тому числі через публікації звітів про конкретні кібератаки і індикаторів компрометації. Цю інформацію можна використовувати для організації захисту комп'ютерних мереж і системної протидії кіберзагрозам національної безпеки держави. Також отримані дані дозволять підвищити рівень обізнаності технічних фахівців органів державної влади». ***(Хакер із Запоріжжя за вказівкою кураторів РФ планував атаку на сайти держорганів України // Дзеркало тижня. Україна (https://zn.ua/ukr/UKRAINE/khaker-iz-zaporizhzhja-za-vkazivkoju-kuratoriv-rf-planuvav-ataku-na-sajti-derzhorhaniv-ukrajini.html). 27.04.2021).***

***

«Україна має багатий досвід протистояння російській кампанії дезінформації, а також кібератакам, і могла би поділитися ним зі Сполученими Штатами, а також з іншими країнами Заходу, щоби посилити ефективність спільної протидії цьому виклику.

Про це заявила посол України в США Оксана Маркарова під час вебінару, організованого Українсько-Американською Діловою радою, передає власний кореспондент Укрінформу.

«У цьому питанні ми в Україні маємо багато чим поділитися. Ми мали справу з великою кількістю кібератак (з боку Росії – ред.) перед тим, як вони були

виявлені тут, у Сполучених Штатах, і ми знаємо, що робити в (таких випадках – ред.)», - зауважила Маркарова.

Вона також зазначила, що Україна застосувала певні заходи для захисту і готова робити це разом зі США, а також іншими країнами Заходу.

«Ми можемо разом скласти план, яким чином підвищити ефективність та дієвість у скоординованому реагуванні на цей виклик»,- підкреслила посол.

Окрім того, за її словами, українська сторона готова розвивати діалог зі США у багатьох інших сферах, у тому числі щодо інновацій та кліматичних змін…» ***(Україна готова поділитися зі США досвідом протистояння російським кібератакам – Маркарова // Укрінформ (https://www.ukrinform.ua/rubric-polytics/3238067-ukraina-gotova-podilitisa-zi-ssa-dosvidom-protistoanna-rosijskim-kiberatakam-markarova.html). 30.04.2021).***

***

Боротьба з кіберзлочинністю в Україні

«Щомісячний рух коштів на рахунках товариств сягав близько 100 млн гривень. Отримані кошти фігуранти витратили на нерухомість, автомобілі, дорогі коштовності та вкладали у свій незаконний бізнес.

Злочинна діяльність групи тривала з 2016 року до моменту її викриття поліцейськими управління протидії кіберзлочинам в Дніпропетровській області, слідчого управління ГУНП області під процесуальним керівництвом Дніпропетровської обласної прокуратури.

Групу організувало колишнє подружжя з м. Верхньодніпровська та 36-річний мешканець м. Дніпро. Через мережу спеціально створених фіктивних суб'єктів господарювання вони проводили безтоварні фінансово-господарські операції. Залучаючи посередників, зловмисники зареєстрували понад 70 підприємств, які не планували реально вести господарську діяльність.

Надалі, використовуючи печатки та реквізити цих товариств фігуранти нібито укладали угоди про постачання товарів, надання послуг та виконання робіт реальним підприємцям та державним установам.

Після надходження безготівкових коштів на рахунки фіктивних підприємств, їх виводили у готівку через банківські картки, оформлені на підставних осіб.

Також поліцейські встановили, що до незаконних оборудок причетні працівники підприємств, що виступали замовниками товарів та послуг, які відповідали за фінансово-бухгалтерську звітність та мали доступи до електронних кабінетів платників податків та систем управління рахунками підприємств. За надання такого роду «послуг» вони отримували певні відсотки від суми перерахованих коштів за кожною фіктивно укладеною угодою. Здебільшого, це були посадові особи сільськогосподарських та фермерських товариств, зареєстрованих на території Дніпропетровської області, а також деяких бюджетних установ.

Фінансово-господарські операції проводилися з використанням програмного забезпечення для подачі податкової звітності «M.E.Doc», а кошти перераховувалися за допомогою системи «Клієнт-Банк».

14 квітня за місцями мешкання, реєстрації фігурантів, в офісних приміщеннях на території м. Дніпро та м. Верхньодніпровськ було проведено 9 обшуків. В результаті правоохоронці вилучили понад 800 тисяч гривень, комп'ютерну техніку, печатки та штампи понад 70-ти створених фігурантами товариств, бухгалтерсько-звітні матеріали фіктивних фінансових операцій, а також банківські картки, використані у злочинній діяльності.

Наразі призначено ряд експертиз, за результатами яких буде визначена спричинена майнова шкода. Поліцейські вживають заходи для встановлення всіх учасників групи. Вирішується питання про повідомлення їм про підозру за ч. 3 ст. 362 (несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї), ч. 2 ст. 366 (службове підроблення), ч. 2 ст. 364 (зловживання владою або службовим становищем), ч. 2 ст. 364-1 (зловживання повноваженнями службовою особою юридичної особи приватного права незалежно від організаційно-правової форми), ч. 4 ст. 190 (шахрайство) Кримінального кодексу України». ***(На Дніпропетровщині поліцейські затримали членів злочинної групи, які організували конвертаційний центр для відмивання грошей // Кіберполіція Національної поліції України (https://cyberpolice.gov.ua/news/na-dnipropetrovshhyni-policzejski-zatrymaly-chleniv-zlochynnoyi-grupy-yaki-organizuvaly-konvertaczijnyj-czentr-dlya-vidmyvannya-groshej-4140/). 16.04.2021).***

***

«Співробітники кіберполіції в Луганській області спільно зі слідчими Старобільського районного управління та колегами з СБУ припинили несанкціоноване втручання в роботу спеціальних радіоелектронних мереж підрозділів сил Операції об'єднаних сил.

В ході проведення слідчо-оперативних дій правоохоронці встановили інтернет-провайдера, який діяв на території м. Старобільськ та радіоелектронне обладнання, яке працювало на радіочастотах спеціального користування і є забороненим для використання цивільними особами.

Під час проведення санкціонованого судом обшуку вилучено радіоелектронне обладнання, що працювало на частотах спеціального користування.

В рамках відкритого кримінального провадження за ст. 361 КК України «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку» під процесуальним керівництвом прокуратури триває досудове слідство». ***(На Луганщині правоохоронці виявили та припинили несанкціоноване втручання в роботу радіоелектронних мереж підрозділів ООС // Кіберполіція Національної поліції України (https://cyberpolice.gov.ua/news/na-luganshhyni-***

pravooxoronczi-vyyavyly-ta-prypynyly-nesankczionovane-vtruchannya-v-robotu-radioelektronnyx-merezh-pidrozdiliv-oos-8266/). 19.04.2021).

***

«Житель столиці скопіював бази даних підприємства для подальшого перепродажу. Збитки нанесені правовласнику можуть сягати більше 2 мільйонів гривень. Фігуранту оголосили про підозру.

Протиправну діяльність 33-річного мешканця Києва викрили співробітники Департаменту кіберполіції спільно з Головним слідчим управлінням Нацполіції.

Чоловік, маючи авторизаційні дані, здійснив несанкціоноване копіювання баз даних та надалі на платній основі надавав доступ до них, розмістивши їх на віддаленому сервері. Бази містили дані щодо фармацевтичного ринку України, їх використовують фармацевтичні компанії для маркетингових досліджень та оцінки ефективності своєї роботи. Зокрема у них містилися відомості про ціни та обсяги роздрібних продажів виробів медичного призначення, косметики, біологічно активних речовин, дитячого харчування, дезінфікуючих засобів.

Фігурант продавав їх за ціною у понад 10 разів меншою від тієї, що пропонував офіційний представник. За попередніми даними, правовласнику нанесено понад 2 мільйони гривень збитків.

Правоохоронці провели обушки за місцем мешкання та роботи фігуранта. Вилучено комп’ютерну техніку, мобільні телефони, «чорнові» записи та гроші. Під час огляду техніки кіберполіцейські виявили копії баз даних, які незаконно збував фігурант.

Правопорушника затримано в порядку ст. 208 Кримінального процесуального кодексу України.

За даним фактом відкрито кримінальне провадження за ч. 3 ст. 190 (Шахрайство), ч. 3 ст. 176 (Порушення авторського права і суміжних прав), ч. 2 ст. 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в комп'ютерах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) Кримінального кодексу України. Фігуранту повідомлено про підозру.

Процесуальне керівництво у кримінальному провадженні здійснює Офіс Генерального прокурора». ***(Кіберполіцейські викрили чоловіка у незаконному збуті баз даних підприємства // Кіберполіція Національної поліції України (https://cyberpolice.gov.ua/news/kiberpoliczejski-vykryly-cholovika-u-nezakonnomu-zbuti-baz-danyx-pidpryyemstva-1480/). 19.04.2021).***

***

«Фігуранти зламували сторінки користувачів соцмереж і від їхнього імені просили друзів про фінансову допомогу. Таким чином вони привласнили понад 500 тисяч гривень.

Злочинну «схему» викрили працівники Департаменту кіберполіції спільно з територіальним підрозділом в Сумській області та працівниками Головного управління Нацполіції області.

П’ятеро місцевих жителів зламували сторінки у соцмережах громадян, використовуючи метод грубого перебору паролів (атаки Brute Force). Крім цього, вони купували у мобільних операторів номери, які перевіряли на верифікацію у соцмережах. В разі, якщо номери були прив’язані до соцмереж, зловмисники використовували функцію відновлення пароля за допомогою SMS.

Отримавши доступ до акаунтів потерпілих, розсилали повідомлення їхнім друзям із проханням позичити гроші. За попередніми підрахунками, у такий спосіб зловмисники привласнили понад пів мільйона гривень.

Правоохоронці провели п’ять обшуків в оселях фігурантів та вилучили мобільні телефони, комп’ютерну техніку, SIM-карти, що використовувалися у протиправній діяльності.

Відкрито кримінальне провадження за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку), ч. 3 ст. 190 (Шахрайство) Кримінального кодексу України. Зловмисникам може загрожувати до восьми років позбавлення волі. Слідство триває.

Процесуальне керівництво здійснює прокуратура Сумської області…». ***(Кіберполіція викрила зловмисників у шахрайстві за схемою «друг просить у борг» // Кіберполіція Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-zlovmysnykiv-u-shaxrajstvi-za-sxemoyu-drug-prosyt-u-borg-6750/). 15.04.2021).***

***

«У результаті злочинної діяльності хакерів фінустанови країн Європи зазнали понад 100 мільйонів гривень збитків. Правоохоронці скерували до суду обвинувальний акт щодо учасника угруповання.

29-річного зловмисника викрили працівники Департаменту кіберполіції спільно з Головним слідчим управлінням Нацполіції в ході міжнародної спецоперації з правоохоронцями Великобританії.

Фігурант приймав замовлення на модифікацію шкідливого програмного забезпечення типу вірусів-шифрувальників, які використовували хакерські угруповання у протиправній діяльності. Потрапивши на комп’ютерну техніку такі програми зашифровують інформацію. Надалі за відновлення доступу до даних зловмисники вимагають викуп.

Атаки хакерів були націлені на фінансові установи країн Європи. За попередніми даними, збитки сягають понад 100 мільйонів гривень.

Крім цього, хакери-вимагачі створювали так звані "сайти витоку інформації", де публікували конфіденційні дані компаній, які відмовлялися платити викуп за розшифровку даних.

За результатами комп'ютерно-технічних експертиз на техніці зловмисника виявлено сотні різноманітних шкідливих програмних продуктів, які модифікувалися та шифрувалися для обходження антивірусних програм.

Хакеру повідомили про підозру за ч. 1 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України.

Підозрюваному загрожує до двох років позбавлення волі. Досудове розслідування завершено, обвинувальний акт скеровано до суду.

Процесуальне керівництво у кримінальному провадженні здійснює Офіс Генерального прокурора України». ***(Учасник міжнародного хакерського угруповання постане перед судом за вірусні атаки на фінустанови // Кіберполіція Національної поліції України (https://cyberpolice.gov.ua/news/uchasnyk-mizhnarodnogo-xakerskogo-ugrupovannya-postane-pered-sudom-za-virusni-ataky-na-finustanovy-3424/). 16.04.2021).***

***

«Слідчі відділення поліції №1 Хмільницького районного відділу поліції спільно з співробітниками кіберполіції задокументували злочинну діяльність 30-річного калинівчанина, який на хакерських форумах продавав паролі доступу до платіжних систем громадян.

За попередньою інформацією, зловмисник за допомогою спеціального програмного забезпечення викрадав паролі до облікових записів платіжних систем та електронних гаманців громадян, формував відповідні електронні бази та продавав їх на форумах. База фігуранта налічувала близько 20 тисяч облікових даних потерпілих.

Під час проведення санкціонованого обшуку за місцем проживання чоловіка поліцейські вилучили комп'ютерну техніку та носії інформації, яку направили на проведення відповідних експертних.

Наразі поліцейські проводять всі необхідні слідчі та процесуальні дії, для встановлення кількості потерпілих та розмір завданої їм шкоди.

Поліцією розслідується кримінальне провадження за ч. 1 ст. 361-2 (несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в комп'ютерах автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) Кримінального кодексу України. Зловмиснику загрожує до двох років позбавлення волі.

Слідчі дії тривають». ***(Поліцейські викрили хакера, який крав паролі до електронних гаманців та платіжних систем громадян // Кіберполіція Національної поліції України (https://cyberpolice.gov.ua/news/policzejski-vykryly-xakera-yakyj-krav-paroli-do-elektronnyx-gamancziv-ta-platizhnyx-system-gromadyan-7585/). 02.04.2021).***

***

«Фігурант розповсюджував шкідливе програмне забезпечення, перебуваючи під вартою. Для цього чоловік створював фіктивні оголошення про продаж товарів та надсилав покупцям у месенджері архівний файл із «вірусом».

Правопорушника викрили співробітники відділу протидії кіберзлочинам Сумщини спільно зі слідчим управлінням обласної поліції та працівниками Сумського слідчого ізолятору.

33-річний фігурант, перебуваючи під вартою, з мобільного телефона розповсюджував шкідливе програмне забезпечення. Для цього чоловік в Інтернеті

створював оголошення про продаж неіснуючих товарів. Потенційному покупцеві пропонував перейти у месенджер для обговорення деталей угоди. У листування зловмисник насилав архівний файл, в якому було зашифровано шкідливе програмне забезпечення. Архів маскував під каталог товарів.

Після потрапляння на пристрій «вірус» збирав авторизаційні дані до онлайн-банкінгу. Надалі зловмисник виводив гроші потерпілих на підконтрольний рахунок.

У ході обшуку в камері засудженого поліцейські вилучили мобільні телефони, що містили докази причетності до правопорушення. Сума збитків встановлюється.

Відкрито кримінальне провадження за ч. 1 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут), ч. 1 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, ч. 3 ст. 190 (Шахрайство), ч. 2 ст. 185 (Крадіжка) Кримінального кодексу України. Вирішується питання про оголошення йому підозри.

Процесуальне керівництво здійснює прокуратура Сумської області». ***(На Сумщині кіберполіція викрила чоловіка у розповсюдженні «вірусу» для привласнення грошей із онлайн-банкінгу // Кіберполіція Національної поліції України (https://cyberpolice.gov.ua/news/na-sumshhyni-kiberpolicziya-vykryla-cholovika-u-rozpovsyudzhenni-virusu-dlya-pryvlasnennya-groshej-iz-onlajn-bankingu-2109/). 01.04.2021).***

***

«…Протиправну діяльність двох чоловіків викрили співробітники відділу протидії кіберзлочинам в Запорізькій області спільно зі слідчими Запорізького районного управління поліції.

Двоє мешканців міста Дніпро віком 21-24 років на замовлення створювали фішингові ресурси для привласнення грошей громадян. Фейкові сайти повністю копіювали дизайн ресурсів майданчиків оголошень та служб доставки. Надалі фігуранти передавали клієнтам посилання на створені фейкові ресурси, де користувачі вводили дані своїх банківських карт. За ці послуги зловмисники отримували близько 70% від суми, що була на банківській картці потерпілих.

Також юнаки методом грубого перебору паролів збирали бази авторизаційних даних користувачів платформ оголошень та служб доставки. Зібрані дані вони перепродавали.

Встановлено, що зловмисники ошукали більше сотні громадян, загальна сума збитків сягає понад 250 тисяч гривень.

В оселях правопорушників поліцейські провели обшуки. Вилучено комп’ютерну техніку та мобільні телефони, банківські картки. До проведення обшуків також було залучено бійців батальйону особливого призначення поліції Запорізької області.

Відкрито кримінальне провадження за ч. 1 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи

мереж електрозв'язку) Кримінального кодексу України. Санкція статті передбачає до трьох років позбавлення волі. Досудове розслідування триває». ***(Кіберполіцейські Запоріжжя викрили двох юнаків у створенні фішингових ресурсів для привласнення грошей громадян // Національна поліція (https://www.npu.gov.ua/news/kiberzlochini/kiberpoliczejski-zaporizhzhya-vikrili-dvox-yunakiv-u-stvorenni-fishingovix-resursiv-dlya-privlasnennya-groshej-gromadyan/). 21.04.2021).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Отримати знання в галузі кібербезпеки, а також консультації юристів і психологів, допомогу в соціальній адаптації, працевлаштуванні й створенні власного бізнесу можуть учасники АТО/ООС з Дніпропетровщини в рамках українсько-норвезького освітнього проекту «Норвегія - Україна.

Професійна адаптація. Інтеграція в державну систему".

Проект для України унікальний. До нього вже приєдналися 24 ветерани регіону. Безплатне навчання протягом трьох місяців вони пройдуть у дніпровському Університеті митної справи та фінансів. Випускники отримають свідоцтво про професійну перепідготовку, загальний сертифікат університету NORD і митної справи та фінансів, а також спільний диплом Міністерства закордонних справ і Міністерства оборони Норвегії». ***(Ігор ТЬОМІН. Дніпропетровщина: Ветеранів навчають кібербезпеки // Голос України (http://www.golos.com.ua/news/134807). 28.04.2021).***

***

Коронавірус COVID-19 та питання кібербезпеки

«По словам Imperva, злонамеренные боты-скальперы накапливали средства индивидуальной защиты от COVID-19 в 2020 году, чтобы получить прибыль от пандемии, и могут нарушить важнейшие цепочки поставок вакцин в этом году.

В отчете Imperva Bad Bot Report от поставщика средств безопасности за 2021 год утверждается, что зафиксирован самый высокий процент вредоносного бот-трафика (26%) с момента публикации отчета в 2014 году. В прошлом году более 40% всех запросов веб-трафика исходили от ботов.

Большая часть (57%) трафика «плохих ботов», наблюдаемого Imperva в прошлом году, была связана с так называемыми «продвинутыми постоянными ботами», которые, по его словам, труднее обнаружить, поскольку они точно имитируют поведение человека. Они были вовлечены в ряд злонамеренных

действий, включая сбор цен, сбор контента, создание и захват учетных записей, мошенничество, отказ в обслуживании и отказ в инвентаризации.

Боты-скальперы начали действовать в конце года, чтобы скупать большие объемы новых игровых консолей, что стимулировало рыночный спрос, прежде чем продавать их с целью получения прибыли. Imperva заявила, что с сентября по октябрь 2020 года трафик плохих ботов на розничные веб-сайты во всем мире вырос на 788%.

Они также активно скупали востребованные продукты, связанные с COVID, такие как маски для лица, дезинфицирующие и моющие средства, а также другие предметы, ставшие популярными в результате пандемии, такие как домашнее тренировочное снаряжение.

Imperva предупредила, что автоматизированные сценарии могут помешать развертыванию вакцины. Он зафиксировал 372% -ное увеличение трафика плохих ботов на веб-сайты здравоохранения с сентября 2020 года и заявил, что по мере того, как вакцины стали широко доступны, показатели выросли до 12000 запросов в час.

По его словам, такие объемы трафика могут перегрузить веб-сайты медицинских организаций, аптек и розничных продавцов, участвующих в развертывании, что затруднит доступ законных клиентов к службам записи на прием.

«Как мы наблюдали в течение последних восьми лет, плохие боты продолжают разорять Интернет, а характеристики атак со временем становятся все более продвинутыми и детализированными», - сказал Эдвард Робертс, директор по стратегии и безопасности приложений в Imperva.

«В течение прошлого года и во время глобальной пандемии они процветали, ориентируясь на новые рынки, и теперь их влияние ощущают обычные потребители. Организации должны предпринимать активные действия для защиты своих веб-сайтов, приложений и API от этих угроз, поскольку боты все чаще участвуют в мошеннических действиях, которые могут стать источником репутационного и финансового ущерба». ***(Phil Muncaster. Bad Bots Could Disrupt #COVID19 Vaccine Rollout // Reed Exhibitions Ltd (https://www.infosecurity-magazine.com/news/bad-bots-could-disrupt-covid19/). 14.04.2021).***

***

«Чуть больше года назад крупные и мелкие предприятия бросили своих сотрудников на удаленную работу, поскольку COVID-19 превратился в полномасштабную пандемию. Теперь, когда исполнилась годовая годовщина эксперимента по работе на дому, компании и даже государственные учреждения манят рабочих вернуться в корпоративные офисы. Это окажет большое и непредсказуемое влияние на многие вещи, включая кибербезопасность.

Аналитики считают, что многие крупные организации, вероятно, подождут до конца этого года, чтобы потребовать некоторых, но не всех сотрудников, вернуться в офис. Однако в конце марта Microsoft взяла на себя инициативу, открыв свою штаб-квартиру в Редмонде, а также несколько соседних кампусов.

Вскоре после этого Amazon отметила, что хочет вернуться к «офисно-ориентированной культуре», когда некоторые сотрудники вернутся к лету.

Не только технологические компании начинают перезванивать сотрудников в офисы. По данным New York Times, мэр Нью-Йорка Билл де Блазио хочет, чтобы муниципальные служащие вернулись в офисы к 3 мая, поскольку право на вакцинацию COVID-19 расширяется.

Не все фирмы (технические или нет) хотят вернуться в офисы. The Wall Street Journal обнаружил, что компании от Salesforce до JPMorgan Chase теряют офисные площади, поскольку видят, что удаленная работа продолжается. Да и сами сотрудники не горят желанием возвращаться в офисы на полную ставку. В июне 2020 года исследование Всемирного экономического форума показало, что трое из четырех хотели сохранить некоторую гибкость в своем расписании.

Все эти факторы приводят к тому, что многие отраслевые обозреватели называют гибридной рабочей силой, когда сотрудники работают из дома и в корпоративном офисе. И хотя этот подход может помочь предприятиям вернуться в нормальное состояние после года травмы, вызванной COVID-19, некоторые аналитики опасаются, что это может привести к другим проблемам, а именно, к еще большей головной боли в области кибербезопасности.

«Когда сотрудники вернутся в офис, наверняка возникнет всплеск проблем, связанных с безопасностью», - сказал Dice Джон Морган, генеральный директор охранной фирмы Confluera. «Организации, однако, должны быть еще более бдительными после того, как волна стихнет, поскольку хакеры теперь закрепились в корпоративной сети и прячутся под покровом».

Директора по информационной безопасности и их группы безопасности продолжают бороться с переходом на работу из дома; кибербезопасность отошла на второй план по сравнению с общим стремлением заставить сотрудников работать как можно быстрее. Это включало большее использование облачных приложений и приложений SaaS, особенно инструментов для совместной работы, а также стремление получить устройства, особенно ноутбуки, в руки сотрудников, не задумываясь обо всех возможных недостатках безопасности.

Эти устройства теперь возвращаются в корпоративные сети после года небезопасной или плохо защищенной работы. В то же время в облако загружается больше данных, которые могут быть загружены в корпоративную или домашнюю сеть со слабыми стандартами безопасности.

«Когда сотрудники вернутся в офис, их способ доступа к своим данным и корпоративным приложениям изменится», - сказал Dice Чарльз Хендерсон, глобальный глава IBM X-Force Red. «Кроме того, сотрудники уже довольно долгое время находятся вдали от централизованных ИТ-функций, и вы не знаете, какой багаж они приносят с собой из дома - от вредоносных программ до недобросовестных практик и плохой гигиены безопасности. Большинству менеджеров по безопасности будет сложно предсказать, как это повлияет на их организацию».

Вот некоторые из проблем кибербезопасности, с которыми сталкиваются большие и малые организации, когда корпоративные двери снова начинают открываться.

Фишинг

За последний год фишинг стал все более серьезной проблемой для руководителей информационной безопасности и их служб безопасности, поскольку мошенники и киберпреступники воспользовались не только плохо защищенными домашними сетями, но также путаницей и неопределенностью, вызванной COVID-19. Эти опасения, в свою очередь, поддаются вредоносным сообщениям и доменам, замаскированным под важные обновления новостей, предупреждения или сайты, предлагающие важную информацию.

В отчете, опубликованном фирмой по безопасности Proofpoint, говорится, что 57 процентов организаций сообщили об успешной фишинг-атаке в 2020 году, что выше 55 процентов, которые сообщили о том же в 2019 году. Во время этих успешных атак 60 процентов организаций сообщили о потере данных, а 52 процента. обнаружил потерю учетных данных или компрометацию учетной записи.

Стивен Банда, старший менеджер по решениям безопасности в Lookout, считает, что рост фишинга, вероятно, продолжится, особенно когда сотрудники будут переключаться между домашней и корпоративной сетями, а мошенники воспользуются преимуществами новой гибридной среды.

«Гибридная рабочая среда предоставляет новый контекст для фишинговых атак», - сказал Банда Дайсу. «Киберпреступники будут использовать этот сценарий гибридной рабочей силы по-разному. Например, маскируясь под менеджера отдела кадров, злоумышленник может запустить фишинговую кампанию, которая включает документ политики удаленной работы. В сообщении может потребоваться, чтобы сотрудники щелкнули ссылку, чтобы принять политику или загрузить документ, который может содержать вирус».

Частично беспокойство связано с возрождением движения BYOD, которое теперь включает удаленных сотрудников, которые возвращают устройства и приложения в корпоративные сети. Это может создать проблемы с директорами по информационным технологиям и их группами безопасности, которые должны управлять личными, а также корпоративными устройствами.

«Удобство использования одного и того же набора устройств для совмещения работы и личной жизни слишком велико, чтобы с ним расстаться. Это означает, что директорам по информационной безопасности необходимо будет инвестировать в кибербезопасность, которая работает как на управляемых, так и на неуправляемых личных устройствах. Эти решения должны будут уважать конфиденциальность пользователей при защите данных организации», - сказал Банда. «Директорам по информационной безопасности также необходимо будет управлять безопасностью для более широкого спектра используемых облачных приложений. В связи со спросом на BYOD организации теперь сталкиваются с проблемой получения информации о приложениях, используемых в их организации».

Он добавил: «С точки зрения мобильных устройств, приложения могут иметь разрешения и возможности, которые не соответствуют требованиям компании. Важное значение будут иметь решения, которые могут идентифицировать приложения, которые содержат уязвимости или представляют риск для организации, и применять политики для ограничения использования».

Безопасный код

Некоторые аналитики безопасности также считают, что появляющаяся гибридная рабочая сила - это время для предприятий и других организаций, чтобы лучше справиться с процессом разработки, включив безопасность в цикл DevOps - другими словами, DevSecOps.

Хотя это не связано напрямую с COVID-19, предполагаемая атака на государство, нацеленная на SolarWinds и ее клиентов (обнаруженная в декабре 2020 года), показала, насколько может быть нарушен процесс разработки и обновления программного обеспечения. Поскольку ожидается, что разработчики будут приходить в офисы, одновременно работая из дома, гибридная модель работы может открыть для специалистов по безопасности возможность занять место за столом разработки приложений. В свою очередь, это может привести к более совершенным методам обеспечения безопасности, внедренным в процесс разработки приложений.

«Безопасность может помочь разработчикам лучше понять качество своего кода - Kubernetes и инструменты безопасности контейнеров могут выявить неправильные настройки в этих критических компонентах разработки, а инструменты безопасности API могут аналогичным образом выявить уязвимости в API компании», - Мишель Маклин, вице-президент компании «Соль безопасности», - сказал Дайс.

«В то же время, когда безопасность обеспечивает эту информацию о состоянии, они также должны поддерживать разработчика с помощью безопасности во время выполнения, выявляя вредоносную активность в производственной среде, чтобы выявлять злоумышленников в действии», - продолжил Маклин. «Миссия безопасности должна охватывать как непосредственную помощь разработчикам в написании более безопасного кода, так и одновременное развертывание активных элементов управления во время выполнения, чтобы предотвратить ошибку разработчика, которая может стоить компании скомпрометированной доступности или кражи данных».

Идентичность - новый периметр

Для некоторых появление гибридной рабочей силы, вероятно, означает конец безопасности периметра. Теперь необходимо сосредоточиться на вопросах идентификации, привилегированного доступа и осознания того, что ни одному человеку или приложению нельзя доверять. Это открывает двери для профессионалов в области безопасности, которые хотят использовать новые стратегии, такие как архитектуры нулевого доверия.

«Организации должны адаптировать и расставить приоритеты для управления и защиты доступа к бизнес-приложениям и данным, например, аналогичным устройствам типа BYOD, а это означает дальнейшую сегрегацию сетей для ненадежных устройств, но с надежными средствами управления безопасным привилегированным доступом для обеспечения производительности и доступа», - сказал Dice Джозеф Карсон, главный специалист по безопасности и консультант по информационной безопасности охранной фирмы Thycotic.

«Организации стремятся к стратегии нулевого доверия, чтобы снизить риски, связанные с гибридной рабочей средой. Это означает, что для достижения

стратегии нулевого доверия организации должны принять принцип наименьших привилегий, который позволяет организациям лучше контролировать права пользователей и приложений, повышая уровень только авторизованных пользователей», - добавил Карсон.

Хендерсон из IBM отметил, что, хотя предприятия могут стремиться к внедрению более новых методов и инструментов безопасности, таких как нулевое доверие или граница службы безопасного доступа (SASE), это долгосрочные проекты безопасности и исправления, которые будут продолжаться независимо от того, как будет выглядеть рабочая сила в будущем. год и далее.

«Переход к нулевому доверию, вероятно, будет проще, но просто сказать, что вы внедряете нулевое доверие, не решит все - это многогранное решение», - сказал Хендерсон. «Организациям необходимо проводить оценки, чтобы увидеть, как выглядит их воздействие - тестируйте, а не угадайте. Как только вы понимаете, что есть проблема, начинать оценивать уже поздно, поэтому ключевым моментом является раннее обнаружение. А поскольку возвращение к нормальной жизни в рабочей силе неизбежно, самое время начать подготовку». ***(What the Hybrid Workforce Means for Cybersecurity Teams // Dice (https://insights.dice.com/2021/04/08/what-the-hybrid-workforce-means-for-cybersecurity-teams/). 08.04.20021).***

***

«За последний год 65% людей во всем мире сообщили, что проводят в Интернете больше времени, чем когда-либо прежде, вероятно, в результате пандемии COVID-19. Поскольку мы подключались к Интернету для всего, от работы и учебы до развлечений, социальных сетей и даже продуктовых магазинов, киберпреступники воспользовались этим и начали скоординированные атаки и убедительное мошенничество.

NortonLifeLock показал, что в прошлом году почти 330 миллионов человек в 10 странах стали жертвами киберпреступлений и более 55 миллионов человек стали жертвами кражи личных данных. Жертвы киберпреступлений вместе потратили почти 2,7 миллиарда часов, пытаясь решить свои проблемы.

Теряю время на киберпреступность

Отчет, проведенный онлайн- опросом Harris Poll среди более чем 10 000 взрослых в 10 странах, включая 1 000 в США, также обнаружил, что 25% американцев обнаружили несанкционированный доступ к учетной записи или устройству за последние 12 месяцев.

Из почти 108 миллионов американцев, которые столкнулись с киберпреступностью за последние 12 месяцев (41%), в среднем 6,7 часов было потрачено на решение возникших проблем, из них, по оценкам, более 719 миллионов часов времени американцы потеряли из-за киберпреступности. С ростом преступной активности в Интернете 47% американцев чувствуют себя более уязвимыми для киберпреступлений, чем до начала пандемии COVID-19.

«Прошедший год был невероятно сложным, поскольку мы справились с эмоциональными и физическими последствиями глобальной пандемии. Более того, существует дополнительная озабоченность по поводу онлайн-здоровья и

безопасности наших семей, поскольку мы проводим больше времени в Интернете», - говорит Пейдж Хэнсон, руководитель отдела обучения кибербезопасности NortonLifeLock. «Киберпреступники воспользовались нашим изменяющимся поведением и увеличением цифрового следа».

Ключевые факторы незащищенности киберпреступности

Увеличение времени пребывания американцев в сети и неспособность отличить факты от вымысла могут быть ключевыми факторами незащищенности их киберпреступности. Семьдесят три процента американцев говорят, что они проводят больше времени в Интернете, чем когда-либо прежде, при этом 59% говорят, что они больше, чем когда-либо раньше, обеспокоены тем, что могут стать жертвой киберпреступности, а 56% признают, что им трудно определить, является ли информация, которую они видят в Интернете, достоверной. из надежного источника. Кроме того, 76% считают, что удаленная работа значительно облегчила хакерам и киберпреступникам использование людей.

«Несмотря на уязвимость и замешательство в этом году, мы начинаем видеть положительную сторону, когда потребители сопротивляются и играют более активную роль в защите своей цифровой жизни», - сказал Хэнсон.

Из-за опасений по поводу киберпреступности 77% американцев заявляют, что они приняли больше мер предосторожности в Интернете. Кроме того, 99% американцев, обнаруживших несанкционированный доступ к учетной записи или устройству за последние 12 месяцев, предприняли некоторые действия для повышения своей кибербезопасности, включая создание более надежных паролей (66%) или обращение в компанию, из которой была взломана учетная запись (51%).

33% обратились за помощью к членам семьи или к Интернету (31%), а 18% вложили больше средств в программное обеспечение для обеспечения безопасности за счет первой покупки или удвоили стоимость ранее существовавших подписок.

Жертвы киберпреступности

Конфиденциальность данных - главная проблема: 88% американцев обеспокоены конфиденциальностью данных и 86% активно предпринимают шаги, чтобы скрыть свой след в Интернете (т. Е. Защитить свою онлайн-деятельность и личную информацию), включая создание более надежных паролей (55%) и ограничение информация, распространяемая в социальных сетях (40%).

Несмотря на усиление мер предосторожности, 40% американцев признают, что не знают, как защитить себя от киберпреступлений. 46% американцев не знали бы, что делать, если их личность была украдена, а 77% хотели бы иметь больше информации о том, что делать, если бы это было.

Молодое поколение менее уверено в решении проблемы кражи личных данных: люди младше 40 лет с большей вероятностью скажут, что они не знали бы, что делать, если их личные данные были украдены (62% против 37%), и что они хотели бы иметь больше информации о том, что делать, если их личные данные были украдены (87% против 70%)». ***(330 million people across 10 countries were victims of cybercrime in 2020 // Help Net Security (https://www.helpnetsecurity.com/2021/04/14/victims-of-cybercrime/). 14.04.2021).***

***

«Отрасли и организации, имеющие решающее значение для борьбы с COVID-19, столкнулись с резким ростом кибератак из-за их быстрого перехода на облачные платформы в свете пандемии.

Когда мир впервые начал обращать внимание на глобальное распространение COVID-19, организации по всему миру внезапно оказались не в состоянии поддерживать типичные методы работы.

Офисы закрывались, навязывались заказы на домработницу, а запросы потребителей часто можно было удовлетворить только с помощью доставки, виртуальных услуг и платформ электронной коммерции.

В результате как крупные предприятия, так и малые и средние предприятия начали быстро переходить с локальных и устаревших систем на облако, чтобы упростить модели удаленной работы и реализовать новые возможности для бизнеса.

По оценкам, расходы на корпоративное облако только во втором квартале 2020 года увеличились на 28% по сравнению с аналогичным периодом прошлого года. Однако, согласно последнему отчету об облачных угрозах Palo Alto Networks, опубликованному во вторник, столь быстрый перенос рабочих нагрузок в облако также означал, что спустя месяцы предприятия изо всех сил пытаются управлять облачной безопасностью и автоматизировать ее - и создали пропасти в безопасности компании. что можно использовать.

Отрасли, имеющие решающее значение для управления COVID-19, особенно пострадали от инцидентов, связанных с безопасностью облачных вычислений. Согласно отчету, больше всего пострадали предприятия розничной торговли, производства и правительства: во время пандемии количество атак увеличилось на 402%, 230% и 205% соответственно.

Неудивительно, что химические производства и научно-исследовательские организации стали ключевыми мишенями для кибератак из-за COVID-19. Яркие примеры включают нападения на производителей вакцин и Европейское агентство по лекарственным средствам (EMA)…

«Эта тенденция неудивительна; эти же отрасли были среди тех, кто сталкивался с наибольшим давлением в плане адаптации и масштабирования перед лицом пандемии - розничные продавцы предметов первой необходимости, а также производство и правительство для поставок и помощи COVID-19», - сообщает Unit 42.. «[..] Хотя облако позволяет предприятиям быстро расширять свои возможности удаленной работы, автоматизированные средства управления безопасностью на основе DevOps и конвейеры непрерывной интеграции / непрерывной доставки (CI / CD) часто отстают от этого быстрого движения».

Однако не все отрасли равны, и некоторые из них добиваются большего успеха, чем другие, в попытках защитить свои облачные рабочие нагрузки.

Управление ведением журнала доступа, ротация ключей доступа и контроль версий в контейнерах облачного хранилища - способ отслеживать изменения, внедрять их и выполнять обслуживание в облачных системах - вот некоторые из методов, которые можно использовать для повышения безопасности облака…

Однако команда обнаружила, что общедоступные облачные системы, в которых может происходить утечка информации, позволяющей установить личность (PII), принадлежащую клиентам или сотрудникам, а также конфиденциальных корпоративных данных, по-прежнему являются проблемой. Цифры высоки: по оценкам, 30% организаций, использующих услуги облачного хостинга, пропускают какой-либо частный контент в Интернете, и проблемы контроля доступа являются причиной такого широкого распространения.

Unit 42 рекомендует компаниям сосредоточиться на обеспечении прозрачности своих облачных рабочих нагрузок, следить за конфигурациями хранилищ, а принятие и обеспечение соблюдения стандартов безопасности в DevOps может снизить угрозу атаки или случайной утечки данных». ***(Charlie Osborne. Industries critical to COVID-19 response suffer surge in cloud cyberattacks // ZDNet (https://www.zdnet.com/article/industries-critical-to-covid-19-response-suffer-surge-in-cloud-cyberattacks/). 06.04.2021).***

***

«На фоне пандемии коронавирусной инфекции (COVID-19) возросло количество кибератака иностранных хакеров на российские научно-исследовательские институты (НИИ), занимающиеся разработкой вакцин от коронавируса, а также военных и авиационных проектов.

Как сообщили изданию «КоммерсантЪ» ИБ-эксперты из компании Group-IB, атаки осуществляются преимущественно злоумышленниками, поддерживаемыми другими государствами, а похищенные данные используется в политических целях. Работа НИИ напрямую связана с конфиденциальной информацией различных отраслей, включая схемы, чертежи изделий и различные закрытые исследования.

Однако в последнее время хакеры действуют не в целях шпионажа, а с намерением нанести ущерб критической инфраструктуре. В сентябре 2020 года сеть одного из институтов была скомпрометирована двумя группировками. Как отметили специалисты, преступники проникли в сеть НИИ в 2017 году и оставалась незамеченными до 2020 года.

Злоумышленники зачастую внедряют сразу несколько вредоносов, выполняющих различные функции, включая банковские трояны, шпионские программы на рабочие устройства или мобильные девайсы сотрудников». ***(Иностранные хакеры стали чаще атаковать российские НИИ // SecurityLab.ru (https://www.securitylab.ru/news/518913.php). 14.04.2021).***

***

«…Министерство здравоохранения штата Вайоминг (WDOH) объявило 27 апреля 2021 года, что он неосторожно подвергается 53 файлов, содержащих COVID-19 и данные испытаний гриппа и 1 файл, содержащий результаты испытаний спирта дыхания. Некоторые файлы были раскрыты еще 5 ноября 2020 года, но WDOH не обнаружил инцидент до 10 марта 2021 года. Согласно WDOH, файлы включали имя или идентификатор пациента, адрес, дату рождения, результаты теста (-ов).) и даты оказания услуги, но не содержали номеров социального страхования, банковской, финансовой или медицинской информации.

Нарушение произошло в результате «непреднамеренного раскрытия» файлов сотрудником WDOH, который по ошибке и недопустимо загрузил файлы в частные и общедоступные репозитории GitHub.com, что привело к их раскрытию неавторизованным лицам. Примечательно, что WDOH предполагал, что GitHub.com, интернет-компания по разработке программного обеспечения, будет использоваться ее сотрудниками только для хранения и обслуживания программного кода.

Непонятно, почему сотрудник WDOH загрузил 54 файла, содержащих данные результатов тестирования пациентов, в том числе результаты тестов на COVID-19, в сервис, предназначенный для хранения данных кодирования. И мы не знаем, прошел ли сотрудник в этом случае обучение по назначению и использованию GitHub.com. Однако, согласно объявлению WDOH, файлы были незамедлительно удалены с GitHub.com, к сотруднику были применены санкции, а WDOH переобучил свой персонал передовым методам обеспечения конфиденциальности и безопасности данных.

Конечно, при обработке личной информации будут происходить ошибки, и никакое обучение не предотвратит все инциденты и утечки данных. Серебряной пули нет. Однако важный вопрос, который должна задать организация, заключается в том, принимаются ли разумные меры для минимизации риска для данных, даже в отношении непреднамеренных ошибок при обработке и использовании систем компании, среди прочего.

Обучение может быть одним из инструментов, которые организации используют для создания культуры конфиденциальности и безопасности. Повышенная осведомленность может помочь свести к минимуму, даже если не устранить, непреднамеренные ошибки. В официальном документе, который мы представили в нашей предыдущей публикации, изложены некоторые соображения по разработке надежной программы, предназначенной для постоянного напоминания сотруднику о бдительности, необходимой для защиты личной информации от несанкционированного доступа, получения, изменения и раскрытия. Это есть и будет постоянной проблемой, особенно в нынешних условиях, когда рабочие места меняются по мере того, как мы выходим из самых тяжелых последствий пандемии». ***(Joseph J. Lazzarotti. DOH Employee Error Causes Breach of COVID-19 and Other Health Data Affecting Nearly 165,000 Individuals // Jackson Lewis P.C. (https://www.workplaceprivacyreport.com/2021/04/articles/training/doh-employee-error-causes-breach-of-covid-19-and-other-health-data-affecting-nearly-165000-individuals/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+WorkplacePrivacyDataManagementSecurityReport+%28Workplace+Privacy%2C+Data+Management+%26+Security+Report%29#page=1). 28.04.2021).***

***

«Борис Джонсон объявил о дорожной карте правительства Великобритании по отмене ограничений на коронавирус для бизнеса и широкой общественности в начале февраля, и с тех пор это вселило надежду для многих по всей стране.

Однако с начала пандемии способ ведения бизнеса навсегда изменился, и многие сотрудники хотят продолжать работать удаленно, поскольку ограничения и ограничения со временем снижаются. Итак, по мере того, как компании расслабляются и правила смягчаются, ожидается, что жизнь вернется к форме «новой нормальной жизни». Но проблемы, связанные с кибербезопасностью, никуда не денутся, и нельзя ослаблять педаль газа, особенно с учетом повышенных рисков, связанных с продолжением удаленной работы.

Во всяком случае, сейчас безопасность должна быть усилена еще больше, чем когда-либо прежде, чтобы обеспечить безопасность всех аспектов бизнеса. Но это не так.

Риск растет

Несмотря на ослабление ограничений на изоляцию, риски кибербезопасности сохраняются и, вероятно, будут расти, поскольку COVID-19 меняет рабочую среду. Поскольку в ближайшие несколько месяцев начнут открываться закрытые помещения, сотрудники захотят выходить на работу в новые помещения, такие как кафе и интернет-кафе. Но работа в открытых сетях и личных устройствах создает незаблокированные шлюзы для кибератак. Поскольку этот гибридный и удаленный способ работы выглядит так, как будто он никуда не денется, компании должны обеспечить наличие необходимой инфраструктуры для борьбы с любыми киберугрозами.

Например, исследование Национального центра кибербезопасности показывает, что за последний год увеличилось количество кибератак, связанных с COVID-19, причем более одной из четырех хакерских атак в Великобритании связано с пандемией. И эта тенденция вряд ли в ближайшее время ослабнет. И в дальнейшем хакеры могут воспользоваться взволнованными путешественниками, ожидающими бронирования следующего отпуска после снятия запрета на поездки, например, путем развертывания поддельных туристических веб-сайтов.

Помимо злоумышленников в этом более широком сценарии, часть проблемы здесь заключается в том, что многие ИТ-команды не используют целостный и многоуровневый подход к безопасности и восстановлению данных, что может привести к разрушительным последствиям, поскольку данные украдены из организаций. Такие проблемы по-прежнему вызывают большой резонанс в компаниях любого размера, поэтому они обращаются за решением к своим MSP.

Важность многоуровневого подхода

Кибербезопасность - это не комплексный подход. Для достижения максимального эффекта требуется полная трилогия решений. Это включает в себя многоуровневую комбинацию сетей DNS, безопасных подключений к конечным точкам, а также образованный и уполномоченный человеческий персонал.

Нельзя игнорировать потребность в безопасности DNS, особенно с ростом числа удаленных сотрудников, чтобы контролировать и управлять политиками доступа в Интернет, а также уменьшать количество вредоносных программ. DNS часто становится мишенью для злоумышленников, поэтому защита на уровне DNS в настоящее время все чаще рассматривается как важный элемент управления безопасностью, обеспечивающий дополнительный уровень защиты между

пользователем и Интернетом путем блокировки вредоносных веб-сайтов и фильтрации нежелательных материалов.

Аналогичным образом, решения для защиты конечных точек предотвращают файловые вредоносные программы, обнаруживают и блокируют вредоносную внутреннюю и внешнюю активность и реагируют на предупреждения системы безопасности в режиме реального времени.

Однако эти инновационные инструменты и решения не могут быть реализованы без Обучение пользователей и внедрение культуры осведомленности о кибербезопасности в персонал. Люди часто являются самым слабым звеном в кибербезопасности, причем 90% утечек данных происходят из-за человеческой ошибки. Таким образом, предлагая правильное обучение и ресурсы, компании могут помочь своим сотрудникам повысить свою киберустойчивость и занять прочную позицию на передовой линии защиты. Эта комбинация имеет решающее значение для обеспечения правильных цифровых решений, а также для лучшего понимания сотрудниками той важной роли, которую они играют в обеспечении безопасности организации. В свою очередь, эти потребности в безопасности предоставляют различные возможности для монетизации канала, поскольку все больше компаний нуждаются в правильном сочетании технологий и образования, чтобы сотрудники могли быть в безопасности.

Роль канала

Компании, особенно малые и средние предприятия, будут обращаться к MSP, чтобы защитить свой бизнес и помочь им достичь киберустойчивости. Это создает уникальную и ценную возможность для MSP проводить клиентов через их пути к кибербезопасности, предоставляя им необходимые инструменты и решения для защиты данных, чтобы максимально использовать возможности домашней рабочей среды своих сотрудников наиболее безопасными способами. Не менее важно, чтобы MSP брали на себя ответственность за обучение своих собственных команд и клиентов. Это включает в себя предоставление дополнительных учебных модулей по онлайн-безопасности посредством постоянного обучения осведомленности о безопасности, а также защиты конечных точек и всего остального, что требуется для повышения киберустойчивости.

Более того, решения и пакеты для обеспечения киберустойчивости могут быть настроены и персонализированы в соответствии с потребностями клиента, включая защиту конечных точек, постоянное обучение конечных пользователей, анализ угроз, а также резервное копирование и восстановление. При наличии правильных инструментов для роста и автоматизации различных услуг, дополненных технической, организационной и личной поддержкой, партнеры по каналам получат ключи к успеху и для развития новых потоков доходов.

Заключение

Хакеры более изобретательны, чем когда-либо прежде, и для борьбы с растущими угрозами предприятиям необходимо оставаться на шаг впереди. Компании должны продолжать учитывать новые реалии удаленной работы и отвлеченной рабочей силы, и они должны убеждать сотрудников в том, что киберустойчивость - это не просто работа ИТ-команд - это ответственность, которую разделяют все. Применяя многоуровневый подход к кибербезопасности,

компании могут разработать целостное представление о своей стратегии защиты с учетом множества векторов доставки современных вредоносных программ и угроз. В рамках этого развивающегося ландшафта кибербезопасности для малых и средних предприятий важно найти партнера MSP, который предлагает разнообразный портфель предложений по безопасности и обучения, а также знания и поддержку для обеспечения безопасности своих бизнес-данных, сотрудников и сети». ***(Steve Law, Kelvin Murray. Cybersecurity Is Not a One-Stop-Shop // Channel Futures (https://www.channelfutures.com/mssp-insider/cybersecurity-is-not-a-one-stop-shop). 23.04.2021).***

***

«…Киберпреступники использовали пандемию COVID-19 для усиления своих атак и создания собственной пандемии. По данным киберотдела ФБР, количество жалоб увеличилось на 400 процентов по сравнению с тем, что они видели до коронавируса.

Эта киберпандемия - лишь одна из многих проблем кибербезопасности, над решением которых работают специалисты RIT в новом Глобальном институте кибербезопасности (GCI).

В конце прошлой осени GCI открыл двери своего ультрасовременного здания площадью 52 000 квадратных футов на территории кампуса. Благодаря институту RIT становится одним из лучших мест в мире для образования, обучения и исследований в области кибербезопасности.

«Возможность работать удаленно и использовать цифровые технологии во всех аспектах нашей жизни имеет огромный потенциал для улучшения мира, но это также действительно открывает поверхность для атак», - сказал Стив Гувер, исполнительный директор Кэтрин Джонсон GCI. «В GCI мы это понимаем и стремимся сделать вас и ваше цифровое Я в большей безопасности».

В основе проблемы кибербезопасности лежит тот факт, что работодатели не могут найти достаточно квалифицированных специалистов для найма более чем на 1 миллион незаполненных рабочих мест в области кибербезопасности по всему миру. RIT работает над тем, чтобы это изменить.

В трехэтажном институте кибербезопасности эксперты собираются вместе, чтобы обучать новых специалистов и студентов, а также расширять границы исследований.

Первый этаж: Центр кибер-обучения

В основе GCI находится Cyber Range and Training Center, виртуальная физическая лаборатория для моделирования сетевых кибератак и сценариев решения проблем.

«Когда вы входите в эту комнату, вы можете почувствовать, на что на самом деле похожа кибератака, - сказал Джастин Пеллетье, директор Cyber Range. «Для экспертов по кибербезопасности и всех, кто участвует в реальных кибератаках, это гигантская песочница, где вы можете подготовиться и тренироваться, не пострадав».

Организаторы GCI в настоящее время создают иммерсивные способы реагирования на инциденты, чтобы организации могли противостоять

продвинутым постоянным угрозам, стремящимся украсть ценную информацию и нанести ущерб.

«Этот опыт будет разнообразным и индивидуальным, поэтому участники никогда не будут знать точно, чего ожидать - как в реальной жизни», - сказал Пеллетье.

Например, участникам может потребоваться защитить сеть медицинского центра во время стихийного бедствия или обнаружить атаку вредоносного ПО, которая может затронуть миллионы розничных клиентов.

Линейка включает 30 компьютерных станций и может одновременно обслуживать более 5000 виртуальных машин. Он имеет видеостену с экранами 1080p и 4K, диспетчерскую, конференц-зал и стены из электростатического стекла.

Светодиодные фонари, окружающие комнату, могут изменить настроение тренировочного сценария от приветливого синего до вызывающего стресс мигающего красного цвета. Грохочущие громкоговорители можно использовать для имитации сценариев стихийных бедствий, а контроль температуры может буквально поднять накал ситуации.

Благодаря вкладу IBM в размере более 3,3 миллиона долларов, киберпространство также было оснащено одними из лучших на рынке продуктов для управления информацией и событиями безопасности (SIEM).

Напротив, Cyber Range находится большой атриум и просторное конфигурируемое пространство для мини-конференций, где GCI может проводить соревнования, беседы, семинары и хакатоны.

На первом этаже также есть секция для обучения широкой общественности вопросам кибербезопасности. В Cyber Experience Center есть экспонаты, посвященные истории кибербезопасности, кибергигиены, исследовательским проектам студентов и преподавателей, а также практическим демонстрациям.

Второй этаж: новое поколение киберзащитников

В этом году в программе RIT по обеспечению компьютерной безопасности для студентов был проведен самый большой за всю историю входящий курс. На втором этаже GCI было создано несколько новых лабораторных помещений, чтобы помочь обучить это новое поколение защитников кибербезопасности.

Ханиф Рахбари, доцент кафедры компьютерной безопасности, этой весной преподает курс беспроводной безопасности в новой лаборатории сетевой безопасности GCI.

«Современный дизайн и новейшее оборудование позволяют проводить более разнообразный набор лабораторных работ, помимо традиционных сетевых лабораторий, что помогает еще больше обогатить образование, получаемое нашими студентами в RIT», - сказал Рахбари. «Теперь у нас есть более удобное пространство для беспроводного оборудования безопасности и сетевого оборудования, программно-конфигурируемых радиомодулей и антенн, среди прочего».

Помимо лаборатории сетевой безопасности, в GCI есть две новые учебные лаборатории по безопасности, а также лаборатория Eaton Cybersecurity SAFE (оценка безопасности и судебная экспертиза). Новая лаборатория Air Gap Lab в здании также дает студентам возможность работать с опасными вредоносными

программами, при этом оставаясь надежно изолированными от остальной части кампуса и Интернета.

Более 500 студентов в настоящее время изучают компьютерную безопасность в RIT, который получил национальное признание за образование и исследования в области кибербезопасности.

На втором этаже отведено место для студентов, обучающихся по программе CyberCorps: Scholarship for Service NSF.

Эти студенты получают стипендию, покрывающую их расходы в RIT, в обмен на согласие работать на государственной должности в области компьютерной безопасности в течение того же количества лет.

В GCI также есть места для студентов, участвующих в соревнованиях, и университетский клуб кибербезопасности RITSEC…

Третий этаж: повышение безопасности программного обеспечения

Третий этаж Глобального института кибербезопасности посвящен исследователям, которые решают некоторые из наиболее актуальных проблем кибербезопасности сегодня и завтра.

Мехди Мирахорли - один из тех исследователей, которые хотят сделать крупномасштабные программные системы более безопасными, быстрыми и надежными.

С момента прихода в RIT в 2014 году Мирахорли, доцент кафедры программной инженерии, работает над анализом и изменением того, как люди создают и поддерживают сложные программные системы. Сегодня, получив более 4 миллионов долларов поддержки от Национального научного фонда, Агентства перспективных оборонных исследовательских проектов (DARPA) и других организаций, Мирахорли и его команда студентов-исследователей работают над изменением культуры разработки.

«Пятьдесят процентов уязвимостей в современных программных системах вызваны недостатками конструкции», - сказал Миракхорли, получивший звание научного сотрудника Kodak Endowed Scholar в Колледже вычислительных и информационных наук Голизано. «Сегодня мы исправляем ошибки безопасности, но не доходим до корня проблемы и не выявляем архитектурные недостатки программного обеспечения».

«Архитектура программного обеспечения выходит за рамки простого кода», - пояснил Мирахорли. Будь то банковская система или электронные медицинские записи, большая часть программного обеспечения требует надежности, доступности, безопасности и производительности. Однако, если части не подходят друг к другу идеально, вся система может рассыпаться.

«Не все программисты - дизайнеры, которые понимают эти важные принципы проектирования программного обеспечения», - сказал Мирахорли. «Однако для того, чтобы стать дизайнером, требуются годы опыта, и они дороги, поэтому у нас их меньше в отрасли».

Вот почему Мирахорли поставил своей долгосрочной целью синтезировать дизайн программного обеспечения во что-то более интуитивное, в частности, для новичков и начинающих программистов.

В 2020 году он получил престижную награду NSF Faculty Early Career Development (CAREER) за свои усилия в области архитектуры программного обеспечения.

Его проект направлен на то, чтобы превратить проектирование и программирование программного обеспечения из чисто ручной и эксклюзивной задачи в задачу, в которой программист и инструмент автоматического синтеза дизайна могут сотрудничать для создания проекта и реализации программного обеспечения, отвечающего его сценариям атрибутов качества.

«По сути, я создаю новый язык программирования, который упрощает людям выражение намерений дизайна», - сказал Мирахорли. «Этот инструмент шаг за шагом проведет программистов по архитектуре и сообщит им, нарушают ли они какие-либо принципы проектирования. Это приведет к меньшему количеству ошибок и проблем с безопасностью».

Например, программисты, которым не терпится добавить логин и пароль в свою систему, могут не знать точно, где разместить свою технологию. Если они обнаружат его на стороне клиента, они могут подвергнуть свою систему уязвимости обхода аутентификации.

Имея под рукой инструмент Мирахорли, программист мог бы получить предупреждение об этой уязвимости и узнать, как ее устранить.

В рамках награды CAREER Мирахорли рассматривает разработку программного обеспечения с когнитивной точки зрения. Он встречается с новыми студентами, начинающими программистами и опытными дизайнерами, чтобы узнать, как разные люди подходят к проблемам архитектуры. Он также занимается разработкой искусственного интеллекта, который может изучать передовой опыт хороших программных систем, существующих сегодня в мире.

В исследовательском пространстве GCI Миракхорли также руководит группой студентов-исследователей, которые создают различные инструменты и методы, которые кодировщики могут использовать для создания более надежного и безопасного программного обеспечения.

«В конечном итоге мы надеемся сделать все наше программное обеспечение безопасным с помощью конструкции», - сказал Мирахорли. ***(Scott Bureau. Cybersecurity complex open for business // Rochester Institute of Technology (https://www.rit.edu/news/cybersecurity-complex-open-business). 28.04.2021).***

***

«По данным местной полиции, коды быстрого ответа (QR), используемые программой отслеживания контактов COVID-19, были захвачены человеком, который просто вбил сверху мошеннические QR-коды, чтобы перенаправить пользователей на веб-сайт против вакцинации.

Теперь ему грозит два обвинения в «препятствовании операциям, проводимым в связи с COVID-19 в соответствии с Законом об управлении чрезвычайными ситуациями», - говорится в заявлении полиции Южной Австралии, в котором объявляется об аресте. Его арест, возможно, просто капля в море: сообщений о том, что другие антиваксовые агенты делают то же самое, есть в большом количестве.

Правоохранительные органы добавили дополнительное предупреждение потенциальным мошенникам с QR-кодами: «Любой человек, уличенный в подделке или создании препятствий для бизнес-QR-кодов, скорее всего, столкнется с арестом и штрафом в размере до 10 000 долларов».

Полиция заявила, что никакие личные данные не были взломаны, но инцидент подчеркивает, что на самом деле все, что нужно злоумышленнику, - это принтер и упаковка этикеток Avery, чтобы нанести реальный ущерб.

В этом случае QR-коды использовались официальным приложением CovidSafe правительства Южной Австралии для доступа к камере устройства, сканирования кода и сбора данных о местоположении в реальном времени, которые будут использоваться для отслеживания контактов в случае вспышки COVID-19, ABC Об этом сообщает News Australia.

Это много личных данных, связанных с одним QR-кодом, которые ждут, когда их украдут.

«В этом случае люди, отсканировавшие незаконный QR-код, были перенаправлены на веб-сайт, распространяющий дезинформацию от антивирусного сообщества», - сказал Threatpost Билл Харрод, вице-президент по государственному сектору Ivanti. «Хотя это вызывает беспокойство, результат мог быть гораздо более опасным».

Использование QR-кода, рост злоупотреблений

Несмотря на очевидную легкость, с которой ими можно злоупотреблять, использование QR-кодов растет. Только в этом месяце Ivanti опубликовал отчет, в котором выяснилось, что 57 процентов респондентов в Китае, Франции, Германии, Японии, Великобритании и США увеличили использование QR-кода с марта 2020 года.

QR-коды стали быстрым бесконтактным способом чтения меню, записи на прием и многого другого с начала пандемии COVID-19. А там, где ценные данные остались незащищенными, киберпреступники обязательно появятся вовремя.

«Известно, что хакеры создают наклейки со злонамеренными QR-кодами и наклеивают их на законные QR-коды, что позволяет им перехватывать транзакции или находиться в процессе их обработки и захватывать платежную информацию», - сказал Харрод.

Ivanti отметила в своем отчете, что этот тип «липкой» вредоносной атаки с помощью QR-кода уже наблюдался, когда она использовалась для кражи платежной информации в таких местах, как рестораны и гаражи. Вредоносные QR-коды также используются для кражи учетных данных при фишинговых и вредоносных атаках.

Ситуация настолько плоха, что Главное подразделение по борьбе с киберпреступностью армии выпустило предупреждение в марте, а также предупредило «пользователей опасаться подозрительных кодов быстрого реагирования».

Армия рекомендовала пользователям избегать сканирования случайных QR-кодов, проявлять особую осторожность при вводе каких-либо учетных данных после сканирования и предлагает, если QR-код накладывается поверх другого, спросить о его законности.

«Проблема в том, что QR-коды по своей конструкции не читаются человеком, и поэтому практически невозможно определить, безопасна ли ссылка, на которую указывает быстро считываемый код, или является вредоносной», - пояснил Харрод в электронном письме. «В течение многих лет мы призывали пользователей узнавать о ссылках, прежде чем они нажимают на них, и искать в URL-адресах контрольные признаки того, что они не заслуживают доверия. Однако с QR-кодами у пользователей нет возможности узнать, прежде чем они будут перенаправлены».

Проверьте QR-коды, ведущие к ссылкам Bit.ly

Харрод сказал, что, основываясь на исследовании Ivanti, пользователи должны предварительно просмотреть все ссылки bit.ly, которые появляются после сканирования QR-кода.

«Bit.ly - это бесплатный сервис сокращения URL-адресов, который также может использоваться хакерами для маскировки вредоносных URL-адресов», - сообщил Харрод. «Хорошая новость в том, что вы можете безопасно предварительно просмотреть ссылку bit.ly, добавив знак плюса (+) в конце URL-адреса. Это направит вас на страницу, отображающую информацию о ссылке, чтобы вы могли определить, законна она или нет».

Он добавил, что, когда это возможно, полностью избегайте угрозы безопасности QR-кодов, открыв браузер и просматривая информацию через корпоративный веб-сайт.

По его словам, также важно, чтобы пользователи понимали средства защиты на своих устройствах, добавив, что Ivanti обнаружила, что 49% пользователей заявили, что не знают, установлены ли у них какие-либо средства защиты.

«Недавнее исследование Ivanti показывает, что пользователи обычно не имеют представления о том, какой тип безопасности существует на их мобильных устройствах, что может создать огромные бреши в безопасности на устройствах, которые также имеют доступ к приложениям и данным компании», - сказал Харрод. «Убедитесь, что на вашем устройстве установлено активное программное обеспечение, которое поможет обнаруживать и устранять вредоносный код и угрозы для мобильного устройства». ***(Becky Bracken. Anti-Vaxxer Hijacks QR Codes at COVID-19 Check-In Sites // Threatpost (https://threatpost.com/anti-vaxxer-hijacks-qr-codes-covid19/165701/). 29.04.2021).***

***

Світові тенденції в галузі кібербезпеки

«…Международные разработки

1. EDPB провела 45-е пленарное заседание и приняла широкий спектр документов.

2 февраля Европейский совет по защите данных провел 45-е пленарное заседание. Он принял заявление по проекту положений протокола к Конвенции о киберпреступности, рекомендации по адекватности ссылок в соответствии с Директивой о правоприменении (LED), заключение по проекту административного

соглашения (AA) для передачи персональных данных между Haut Conseil du Commissariat aux Comptes (H3C) и Совет по надзору за бухгалтерским учетом публичных компаний (PCAOB), а также ответ на анкету Европейской комиссии по обработке персональных данных для научных исследований с упором на исследования, связанные со здоровьем. EDPB также провел обмен мнениями о недавнем обновлении Политики конфиденциальности Whatsapp.

2. EDPS опубликовала заключения о Законе о цифровых услугах и Законе о цифровых рынках.

10 февраля Европейский надзорный орган по защите данных (EDPS) опубликовал заключения по Закону о цифровых услугах и Закону о цифровых рынках. Он направлен на защиту основных прав людей, включая защиту данных. Что касается Закона о цифровых услугах, EDPS рекомендовала дополнительные меры для лучшей защиты людей в отношении модерации контента, таргетированной онлайн-рекламы и рекомендательных систем, используемых онлайн-платформами, такими как социальные сети и торговые площадки. Что касается Закона о цифровых рынках, он рекомендовал регулировать крупные онлайн-платформы, продвигать справедливые и открытые цифровые рынки и справедливую обработку персональных данных, чтобы способствовать развитию конкурентных цифровых рынков, чтобы предоставить людям дополнительный выбор.

3. В Германии принят законопроект о защите данных в телекоммуникациях и телемедиа.

10 февраля Федеральный кабинет министров Германии принял проект закона о защите данных и конфиденциальности в телекоммуникациях и телемедиа. Он планирует заменить существующие положения Закона о телекоммуникациях 2004 года и Закона о средствах массовой информации 2007 года и реализовать Директиву о конфиденциальности и электронных коммуникациях (2002/58 / EC). Проект включает положения о конфиденциальности связи, данных о местоположении, отображении и подавлении идентификаторов вызывающих абонентов, справочниках конечных пользователей, технических и организационных мерах предосторожности, согласии на хранение информации в оконечном оборудовании и штрафах.

4. Вьетнам опубликовал проект указа о защите персональных данных для общественного обсуждения.

9 февраля Министерство общественной безопасности Вьетнама опубликовало вторую версию проекта указа о защите персональных данных. Он планирует установить более строгие правила и предоставить положения о конкретных правах субъектов данных, трансграничной передаче данных и обработке конфиденциальных личных данных. Нарушение может повлечь временную приостановку работы, отзыв разрешения на трансграничную передачу данных и денежные штрафы.

5. Вирджиния приняла Закон о защите данных потребителей.

2 марта губернатором был подписан Закон Вирджинии о защите данных потребителей (CDPA), который вступит в силу 1 января 2023 года. Закон CDPA устанавливает права потребителей Вирджинии на контроль того, как компании

используют личные данные физических лиц. Он предусматривает, что компании должны защищать личные данные, которыми они владеют, и отвечать потребителям, осуществляющим свои права.

6. Датские органы по защите данных опубликовали краткое руководство по настройке файлов cookie.

12 февраля Совет по цифровой безопасности, Управление бизнеса Дании и Агентство по защите данных Дании опубликовали краткое руководство по использованию файлов cookie. Краткое руководство можно использовать в качестве контрольного списка для организаций, устанавливающих файлы cookie, с указанием того, как соблюдать правила размещения файлов cookie Директивы об электронной конфиденциальности и правила обработки связанных с ними персональных данных Положения о защите данных.

7. UK ICO опубликовал набор инструментов для анализа данных.

17 февраля Управление комиссара по информации Великобритании (ICO) опубликовало Toolkit для организаций, рассматривающих возможность использования аналитики данных. Его цель - помочь распознать риски для прав и свобод людей, создаваемые использованием аналитики данных, с самого начала жизненного цикла проекта аналитики данных. Инструментарий начинается с вопросов для определения правового режима, включая законность, подотчетность и управление, принципы защиты данных и права субъектов данных. Затем он создаст отчет, содержащий индивидуальные рекомендации для конкретного проекта анализа данных». ***(Mark Robinson, Nanda Lau, James Gong. China – Cyber security and data protection April round up // Herbert Smith Freehills (https://hsfnotes.com/data/2021/04/12/china-cyber-security-and-data-protection-april-round-up/#page=1). 12.04.2021).***

***

«Новое исследование, опубликованное сегодня Всемирным экономическим форумом (ВЭФ), выявило необходимость унификации практики кибербезопасности в авиационном секторе.

В исследовании «Пути к киберустойчивой авиационной отрасли» описывается, как авиакомпании, аэропорты и производители самолетов в настоящее время используют разные подходы к противодействию киберрискам. Он включает предупреждение о том, что растущие уровни взаимозависимости внутри отрасли «могут привести к системным рискам и каскадным эффектам».

Чтобы защититься от этих рисков, ВЭФ связался с руководителями 50 организаций, включая ACI, EASA, IATA и Eurocontrol, чтобы определить, как авиационный сектор может подготовиться к будущим инцидентам безопасности и кибератакам.

Коалиция призвала к глобальному принятию девяти принципов, которые она разработала для унификации требований безопасности во всей отрасли.

На международном уровне коалиция хотела бы, чтобы правила были согласованы на глобальном уровне и были разработаны международные стандарты обмена информацией. Он также призвал к созданию системы беспристрастной

оценки и сравнительного анализа и базовых показателей киберустойчивости в цепочке поставок и добавленной стоимости.

На национальном уровне группа хочет, чтобы была возможна переподготовка и поощрялось более открытое общение в отношении авиационных происшествий.

Организационные приоритеты, сформулированные коалицией, включали интеграцию киберустойчивости в практики обеспечения устойчивости бизнеса, улучшение сотрудничества и необходимость обеспечения оценки рисков и определения приоритетов в отношении кибербезопасности.

«Авиационная отрасль имеет большой опыт в области безопасности, устойчивости и защиты от физических угроз и должна интегрировать киберриски в эту культуру безопасности и устойчивости», - сказал Жорж Де Моура, руководитель отраслевых решений Центра кибербезопасности Всемирного экономического центра. Форум.

«Общее понимание и подход к существующим и возникающим угрозам позволит отрасли и государственным субъектам принять подход к кибербезопасности с учетом рисков для обеспечения безопасной и устойчивой авиационной экосистемы».

Крис Вердонк, партнер Deloitte, Бельгия, сказал, что установление доверия между межотраслевыми организациями и национальными и наднациональными властями, а также принятие совместной позиции киберустойчивости будет «логическим, но сложным следующим шагом» для авиационной отрасли.

Он добавил: «Однако, если усилия не будут коллективными, киберриски сохранятся для всех. Дальнейшее укрепление обширного и инклюзивного сообщества, а также разработка и внедрение базовой линии безопасности - ключ к адаптации к нынешней цифровой реальности». ***(Sarah Coble. Aviation Industry Lacks Cohesive Cybersecurity Approach // Reed Exhibitions Ltd (https://www.infosecurity-magazine.com/news/aviation-industry-wef-study/). 14.04.2021).***

***

«Рынок глобальной кибербезопасности услуг будет стоить $ 192.7bn через семь лет, согласно новому отчету по Grand View Research, Inc.

Исследователи полагают, что размер рынка, который в 2020 году оценивается в 91,15 миллиарда долларов, с 2021 по 2028 год будет увеличиваться при среднегодовом темпе роста (CAGR) 10,2%.

Факторы, которые, как ожидается, будут стимулировать рост размера рынка, включают прогнозируемое продолжение нарушений кибербезопасности, затрагивающих предприятия и отдельных лиц и подпитывающих необходимость устранения уязвимостей в сетях, приложениях и системах.

Ожидается, что распространение смартфонов и продолжающееся развертывание высокоскоростных интернет-сетей приведет к росту рынка услуг кибербезопасности, инициируя принятие мобильных приложений для всего, от банковского дела до мониторинга здоровья и общения.

«Все эти приложения также стали потенциальными целями для хакеров, тем самым побуждая компании выбирать услуги кибербезопасности, чтобы выявлять

лазейки в приложениях, закрывать лазейки и впоследствии спасать пользователей от потенциальных потерь», - отмечают исследователи.

Другие ожидаемые драйверы роста рынка, отмеченные в отчете, включают необходимость соблюдения различных нормативных актов и стандартов, таких как HIPAA, FISMA и PCI DSS.

Основные прогнозы отчета заключаются в том, что отрасль здравоохранения, которая с 2016 года потеряла 160 миллионов долларов только из-за атак программ-вымогателей, будет демонстрировать самый высокий среднегодовой темп роста в 11,4% за прогнозируемый период.

«Участившиеся случаи киберпреступлений в недавнем прошлом, и особенно во время вспышки пандемии COVID-19, побудили разработчиков медицинских приложений устранить уязвимости приложений», - отмечают исследователи.

Они добавили: «Ожидается, что киберпреступления против отрасли здравоохранения будут усиливаться в связи с продолжающейся цифровизацией и внедрением медицинских устройств на основе Интернета вещей».

Ожидается, что Азиатско-Тихоокеанский регион возглавит региональный рост как наиболее быстрорастущий регион за прогнозируемый период с прогнозируемым среднегодовым темпом роста более 16,3%.

Исследователи писали: «Ожидается, что Азиатско-Тихоокеанский регион предложит многочисленные возможности для внедрения услуг кибербезопасности, учитывая продолжающуюся цифровизацию в Индии, Малайзии, Таиланде и странах Юго-Восточной Азии».

Grand View Research - это калифорнийская исследовательская и консалтинговая компания со штаб-квартирой в Сан-Франциско, в состав которой входят более 425 аналитиков и консультантов». ***(Sarah Coble. Cybersecurity Services Market to be Worth $192.7bn // Reed Exhibitions Ltd (https://www.infosecurity-magazine.com/news/cybersecurity-services-market-to/). 13.04.2021).***

***

«В связи с тем, что во время пандемии Covid-19 удаленная работа значительно возросла, кибербезопасность становится все более сложной. Согласно отчету о стоимости утечки данных за 2020 год от консалтинговой фирмы Capita, удаленная рабочая сила увеличила среднюю общую стоимость утечки данных почти на 137000 долларов. Дэнни Дженкинс, генеральный директор поставщика технологий безопасности ThreatLocker, считает, что лучший способ борьбы с этим - политика нулевого доверия.

«Концепция нулевого доверия в основном означает, что нужно начинать без доверия и применять доверие только там, где это необходимо», - говорит он. «Каждый раз, когда вы открываете программу на своем компьютере, она получает доступ ко всем данным, к которым у вас есть доступ. Мы предполагаем, что эти приложения не собираются красть наши данные, и внушаем им доверие, но иногда они становятся скомпрометированными.

«Реализуя стратегию нулевого доверия, мы останавливаем работу приложений, которые не нужны бизнесу. Философия заключается в том, чтобы

разрешать только то, что необходимо, а не разрешать все, а затем пытаться искать те вещи, которые могут быть проблематичными позже».

Несмотря на широкое распространение на наших устройствах и репутацию универсального решения для кибератак, Дженкинс говорит, что организациям не следует полагаться исключительно на антивирусное программное обеспечение для обеспечения своей кибербезопасности.

«Антивирусное программное обеспечение, по сути, пытается понять, хорошо что-то или плохо, а затем блокировать плохое», - объясняет он. «Они делают это, полагаясь на черный список и используя прошлый опыт для создания правил, определяющих приложения как плохие. Но это создает проблемы по двум причинам.

«Во-первых, если антивирусное программное обеспечение решает, что, например, синхронизация с Интернетом означает надвигающуюся кибератаку, тогда оно блокирует законные инструменты синхронизации файлов. Антивирусу очень сложно отличить что-то вроде Dropbox от специальной вредоносной программы. Они делают то же самое, а иногда и с одним и тем же кодом. По сути, это часто не удается».

Дженкинс говорит, что другая проблема антивирусного программного обеспечения заключается в том, что оно не может предотвратить атаки, которые превращают «безопасные» приложения в оружие. «Например, кто-то недавно взломал компанию водоснабжения во Флориде и изменил уровень хлористого водорода до 11 000 частей на миллион, что по сути является ядом», - говорит он. «Они сделали это с помощью программного обеспечения для удаленного доступа. Им не требовалось вредоносное ПО, поэтому антивирус его не обнаружил».

Киберпреступники постоянно меняют свою тактику и, используя атаки нулевого дня, используют программное обеспечение до или после выпуска патча.

«Об этих атаках обычно становится известно до того, как программа была исправлена», - говорит Дженкинс. «Многие киберпреступления связаны с тем, что провайдеры не устанавливают исправления в свои системы. Но когда у вас есть атака нулевого дня, неважно, насколько хороша ваша кибергигиена, насколько хорошо вы исправляете свои системы, вы все равно уязвимы».

Но организации могут снизить риск этих атак.

«Хотя такие атаки существуют, вы все равно должны исправлять свои системы, чтобы избежать атак ненулевого дня», - говорит Дженкинс. «Но вы всегда должны предполагать, что ваша сеть и инфраструктура скомпрометированы, и вводить элементы управления внутри вашей среды, которые ограничивают движение, когда кто-то входит».

В начале 2020 года американская компания-разработчик программного обеспечения SolarWinds стала жертвой кибератаки, которая распространилась на ее клиентов. Для клиентов, которые использовали Ringfencing для приложений SolarWinds, атака была ограничена активами, к которым они могли получить доступ внутри их сетей.

«Если вы ограничиваете возможности приложения, при его взломе размер потенциального ущерба ограничивается тем, к чему ему нужно получить доступ», - говорит Дженкинс. «Так, например, если бухгалтерское программное обеспечение

QuickBooks скомпрометировано и у него есть доступ только к базе данных QuickBooks, то это единственное, что оно может повредить. Ограничьте то, что приложение может делать на нескольких уровнях, и вы действительно сможете усилить свою атаку.

«Не доверяйте ничему, кроме того, что он должен делать, и тогда, когда вы попадете в брешь, ваша брешь будет настолько незначительной, что не имеет значения. Если вы применяете открытый подход, нарушения приводят к прекращению бизнеса. Наиболее вероятный способ выйти из бизнеса в 2021 году - это кибернетическая утечка».

ThreatLocker помогает своим клиентам внедрить эти протоколы безопасности.

«Мы существуем для того, чтобы довести эти элементы управления с нулевым доверием, которые ранее были доступны только для очень крупных предприятий, на конечную точку», - говорит Дженкинс. «У малого бизнеса или у поставщика управляемых услуг много клиентов, на которых установлено различное программное обеспечение и обновляется по собственному расписанию. На этом этапе нулевое доверие становится очень сложным, потому что теперь вам нужно беспокоиться обо всех этих обновлениях.

«Мы взяли эту концепцию нулевого доверия и создали предопределенные параметры того, что требуется для запуска таких программ, как Windows или Microsoft Office, чтобы клиенту не нужно было беспокоиться, если различные обновления будут заблокированы».

ThreatLocker Ringfencing защищает приложения, так что они не могут отрицательно взаимодействовать с другими частями системы.

«Мы разделяем эти атаки на части, поэтому, если есть уязвимость в программном обеспечении, если есть уязвимость нулевого дня, вероятность эффективной атаки значительно, если не полностью, снижается. Мы даем клиентам новый уровень видимости и контроля». ***(Elly Yates-Roberts. The importance of zero-trust policies in cybersecurity // Tudor Rose (https://www.technologyrecord.com/Article/the-importance-of-zero-trust-policies-in-cybersecurity-121665). 15.04.2021).***

***

«Люди говорят о рынке труда в сфере кибербезопасности, как о монолите, но в рамках кибербезопасности существует ряд различных ролей, зависящих не только от уровня ваших навыков и опыта, но и от того, что вы любите делать.

Фактически, Cybercrime Magazine представил список из 50 наименований должностей, связанных с кибербезопасностью, а CyberSN, рекрутинговая организация, представила собственный список из 45 категорий должностей, связанных с кибербезопасностью.

Точно так же OnGig.com, компания, которая помогает фирмам писать объявления о вакансиях, проанализировала 150 наименований вакансий в области кибербезопасности и составила свой собственный список 30 лучших. Эта статья основана на исследовании, которое я провел с помощью Springboard, одного из

первых учебных курсов по кибербезопасности с гарантией работы и наставничеством 1: 1.

В частности, CyberSeek.org, совместная отраслевая инициатива, посвященная рынку труда в сфере кибербезопасности, предлагает интерактивный список не только различных должностей в сфере кибербезопасности, но и предлагает вам карьерный путь, показывающий, как вы можете получить повышение.

Сложность заключается в том, что эти названия и роли обычно не стандартизированы, плюс они постоянно меняются по мере развития самой отрасли. Национальный институт науки и технологий в рамках своей Национальной инициативы по обучению в области кибербезопасности пытается стандартизировать должности, используя следующие понятия:

Задачи (действие, выполняемое человеком)

Знания (понятия, которые должен знать человек)

Навыки (способность выполнять действие)

Организации могут использовать эти концепции для создания ролей и команд для выполнения необходимых им задач.

Следует иметь в виду еще кое- что: согласно данным опроса SOC Skills Survey от Cyberbit 2020, отделы кадров могут не понимать рынок труда в области кибербезопасности или то, как нанимать людей в этой области.

Здесь мы должны провести несколько различий. Роли в сфере кибербезопасности различаются по уровню необходимого опыта, а также от того, являетесь ли вы красной командой (наступление) или синей командой (защитой). Наступательные роли (например, тестеры на проникновение), как правило, требуют большего опыта по мере того, как вы углубляете свое понимание защитной практики.

Итак, какие должности в сфере кибербезопасности наиболее распространены и чем они отличаются друг от друга?

Еще несколько должностей начального уровня, обычно требующих сертификации, например, CompTIA Security +, включают:

Аналитик по кибербезопасности: аналитик по кибербезопасности отвечает за защиту сетей и данных компании. Помимо управления всеми текущими мерами безопасности, аналитик также отвечает за реагирование на нарушения безопасности и защиту оборудования компании, например, компьютеров сотрудников.

Инженер по безопасности: Инженеры по безопасности должны планировать и выполнять стратегию информационной безопасности компании и поддерживать все решения безопасности. Они также могут нести ответственность за документирование состояния безопасности своей компании и любых проблем или мер, принимаемых под их контролем. Инженеры по безопасности, как правило, занимают более оборонительную позицию, чем их коллеги-аналитики.

Консультант по безопасности: Консультант по безопасности отвечает за оценку состояния безопасности компании на контрактной основе, а также выступает в качестве советника для других ИТ-сотрудников. Целью консультанта является управление угрозами, и он часто будет планировать, тестировать и управлять начальными итерациями протоколов безопасности компании.

Консультанты, как правило, находятся вне организации, в то время как аналитики по кибербезопасности будут внутренними.

Больше ролей среднего уровня и больше агрессивных ролей, обычно требующих сертификации, такой как Certified Ethical Hacker, включают:

Advanced Threat Analyst: продвинутый аналитик угроз будет отслеживать компьютерные сети с целью предотвращения несанкционированного доступа к файлам и системам. Они также предоставляют отчеты высшему руководству, касающиеся возможностей технической защиты компании.

Оценщик информационной безопасности: Оценщик информационной безопасности рассматривает и дает рекомендации относительно состояния безопасности компании. Для этого они проводят собеседования с ИТ-сотрудниками, проверяют безопасность сети и тестируют уязвимости. Оценщик также проверяет политику и процедуры безопасности компании.

Тестер на проникновение: Тестер на проникновение нанят для легального взлома компьютерных сетей компании. Тестировщики также могут использовать тактику социальной инженерии и пытаться получить информацию, притворяясь на словах человеком, которому доверяют. При обнаружении уязвимостей тестер на проникновение даст рекомендации по повышению безопасности.

Должности более высокого уровня, обычно требующие сертификации, например, сертифицированного специалиста по безопасности информационных систем (CISSP) и не менее пяти лет опыта, включают:

Информационная безопасность Аналитик: аналитик информационной безопасности отвечает за защиту корпоративной сети и поддержания всех средств защиты от нападения. Аналитик может также реализовать план аварийного восстановления компании в случае сбоев в сети. Между прочим, согласно OnGig, это наиболее востребованная работодателями инструкция по кибербезопасности.

Менеджер информационной безопасности: Менеджер информационной безопасности разрабатывает политики и процедуры, направленные на обеспечение безопасности сети компании. Они наблюдают за аналитиками информационной безопасности, гарантируя, что компания соблюдает стандарты и нормы информационной безопасности. Как менеджер, они отвечают за прием на работу и обучение новых аналитиков по информационной безопасности.

Наконец, есть директор по информационной безопасности. Это руководящая должность среднего уровня, которая часто подчиняется главному техническому директору, главному информационному директору, финансовому директору или даже главному исполнительному директору и часто представляет собой конечную цель карьерного роста в сфере кибербезопасности.

Директор по информационной безопасности (CISO) отвечает за общий план безопасности компании. В конечном итоге они несут полную ответственность за нарушения сетевой безопасности и работают с другими руководителями, чтобы гарантировать, что отделы соблюдают стандарты безопасности.

Как видите, существует множество возможных названий должностей, связанных с кибербезопасностью, и важно знать самые распространенные из них. В то же время также важно обращать внимание на то, как конкретная компания определяет роль, чтобы вы в итоге оказались на подходящей для вас работе…»

(What are the different roles within cybersecurity? // The Hacker News (https://thehackernews.com/2021/04/what-are-different-roles-within.html). 17.04.2021).

***

«Недавно TalentLMS в партнерстве с Kenna Security опросила 1200 сотрудников об их привычках к кибербезопасности, знании передовых практик и способности распознавать угрозы безопасности. Вот некоторые из ошеломляющих результатов, которые предлагают некоторое объяснение того, почему киберпреступность превратилась в такой прибыльный бизнес:

69% респондентов прошли обучение по вопросам кибербезопасности у своих работодателей, и все же, когда их попросили пройти базовую викторину, 61% не смогли

Только 17% опрошенных сотрудников информационных служб прошли викторину по сравнению с 57% работников здравоохранения.

59% сотрудников прошли обучение по кибербезопасности в связи с ростом удаленной работы в результате пандемии COVID-19.

60% сотрудников, не прошедших тест по кибербезопасности, сообщают, что чувствуют себя в безопасности от угроз.

Больше сотрудников хранят свои пароли в виде открытого текста, чем те, кто хранит их в менеджерах паролей.

Сотрудники офиса сообщают, что чувствуют себя в большей безопасности от угроз кибербезопасности, чем удаленные, но имеют гораздо худшие привычки к обеспечению безопасности.

Эксперты предлагают советы о том, как улучшить инициативы по обучению кибербезопасности для достижения лучших результатов.

Эти ошеломляющие результаты приводят к выводу, что просто наличия программы обучения кибербезопасности недостаточно. Большинство сотрудников также сообщают, что их компании внедрили правильные фундаментальные меры безопасности, обеспечивающие существенную защиту от угроз кибербезопасности:

66% требуют, чтобы сотрудники использовали двухфакторную аутентификацию

67% имеют установленную политику сообщения об утерянных и украденных устройствах.

75% требуют обязательной периодической смены пароля

Несмотря на эти цифры, не секрет, что целеустремленные хакеры намного опережают меры защиты, введенные компаниями, и еще многое предстоит сделать. «Эти результаты опроса показывают, что, хотя большинство опрошенных сотрудников показывают, что их компании движутся в правильном направлении, существует большое количество компаний, которые не проводят базовое обучение кибербезопасности (31%) или не предлагают многофакторную аутентификацию для своих систем. (от 18 до 34%). Эти пробелы в базовой гигиене кибербезопасности - это то, что часто используют злоумышленники, и это хорошее напоминание, что нам еще предстоит проделать большую работу», - говорит

Джерри Гамблин, директор по исследованиям в области безопасности Kenna Security.

Янив Бар-Даян, генеральный директор и соучредитель Vulcan Cyber, говорит: «На протяжении десятилетий мы довольно хорошо выявляли и определяли приоритеты угроз и уязвимостей кибербезопасности, однако мы все еще пытаемся проактивно координировать усилия по устранению проблем, которые мы найти. Идентификация - это только начало, и, как показывает новое исследование, индустрии кибербезопасности предстоит проделать большую работу. Наша неспособность исправить ситуацию становится еще хуже, прежде чем она станет лучше, особенно потому, что векторы атак продолжают развиваться, в то время как мы изо всех сил пытаемся защитить людей, процессы, цепочки поставок и используемые технологии. Чтобы обезопасить все движущиеся части нашей новой цифровой реальности, необходимы согласованные усилия, предпринимаемые на высшем уровне».

«Быстрый переход за последний год к модели удаленной работы увеличил нагрузку на весь ИТ-персонал. Даже с ИТ-персоналом, хорошо разбирающимся в облачных сервисах и поддерживающем виртуальную рабочую силу, они больше не могут эффективно использовать свой опыт, учитывая дополнительную рабочую нагрузку, - говорит Брендан О'Коннор, генеральный директор и соучредитель AppOmni. - Организациям следует подумать о сбалансированном подходе. обучать своих сотрудников и вкладывать средства в средства автоматизации. Нет необходимости в обширном обучении и круглосуточном ручном мониторинге, когда правильные инструменты автоматизации могут дополнять ИТ-персонал по мере того, как он наращивает свои навыки». ***(Cybersecurity training lags, while hackers capitalize on the pandemic // BNP Media (https://www.securitymagazine.com/articles/95011-cybersecurity-training-lags-while-hackers-capitalize-on-the-pandemic). 14.04.2021).***

***

«Vanson Bourne по заказу компании Trend Micro провела онлайн-опрос 500 специалистов по ИТ и ОТ (операционные технологии) в США, Германии и Японии. Опрос показал, что примерно трое из пяти (61%) производителей сталкивались с ИБ-инцидентами, причём в большинстве случаев (75%) их результатом стали системные сбои. Чаще, чем в двух случаях из пяти (43%), перебои в работе длились более четырёх дней.

«Производственные организации по всему миру удваивают скорость цифровой трансформации, чтобы улучшить работу “умных” фабрик. Разрыв в осведомлённости о кибербезопасности в ИТ и ОТ приводит к дисбалансу между людьми, процессами и технологиями, что даёт злоумышленникам возможность проводить атаки, — говорит Акихико Омикава (Akihiko Omikawa), исполнительный вице-президент Trend Micro по безопасности интернета вещей. — Именно поэтому компания Trend Micro объединила ИТ- и ОТ-аналитику и предлагает комплексное решение “от цеха до офиса”. Мы помогаем вернуть видимость и постоянный контроль в руки владельцев “умных” фабрик».

Согласно результатам опроса во всех трёх странах, технологии (78% опрошенных) рассматриваются как самая большая проблема безопасности, хотя люди (68%) и процессы (67%) также входят в число основных проблем. При этом менее половины участников опроса заявили, что принимают технические меры для повышения уровня кибербезопасности.

Визуализация активов (40%) и сегментация (39%) — меры кибербезопасности, вероятность реализации которых самая низкая. Это свидетельство того, что такие меры — наиболее технически сложные для выполнения. Организации с высокой степенью сотрудничества ИТ- и ОТ-направлений с большей вероятностью внедрят технические меры безопасности, чем организации с меньшей сплочённостью. Особенно большая пропасть пролегла между организациями с высоким уровнем сотрудничества ИТ–ОТ и организациями, практически не практикующих такое сотрудничество, в использовании межсетевых экранов (66% против 47%), систем предотвращения вторжений (62% против 46%) и сегментации сети (54% против 37%).

Стандарты и методические рекомендации были названы основным фактором расширения сотрудничества и в США (67%), и в Германии (51%), и в Японии (57%). Самыми популярными директивами в этой области стали Концепция кибербезопасности (Cyber Security Framework) американского Национального института стандартов и технологий (NIST) и стандарт ISO27001 (в отношении Системы менеджмента информационной безопасности — СМИБ), разработанный совместно Международной организацией по стандартизации и Международной электротехнической комиссией.

Самым распространённым организационным изменением, о котором говорили производители во всех трёх странах, было назначение директора по безопасности.

Trend Micro рекомендует трёхэтапный технический подход к обеспечению безопасности «умных» фабрик и поддержанию их работоспособности:

предотвращение за счёт снижения рисков вторжения в такие точки обмена данными, как сеть и демилитаризованная зона (DMZ). Эти риски могут включать использование USB-устройств для хранения данных, ноутбуков, привезённых на завод третьими лицами, шлюзы интернета вещей;

обнаружение аномального поведения сети, например, общения с сервером Command & Control (C&C) и множественных сбоев входа в систему. Чем раньше происходит обнаружение, тем проще и быстрее можно остановить атаки с минимальным воздействием на деятельность организации;

постоянство имеет решающее значение для защиты «умных» фабрик от любых угроз, которые были пропущены на этапах предотвращения и обнаружения. Решения Trend Micro TXOne Network для защиты промышленных сетей и конечных точек специально созданы для сред ОТ: они работают в широком диапазоне температур, просты в использовании и минимально влияют на производительность». ***(Кибератаки на «умные» фабрики могут остановить производство на несколько дней // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5727757-Kiberataki-na-umnye-fabriki-mogut.html). 06.04.2021).***

***

«За последние два года более 80% компаний подверглись хакерским атакам на микропрограммное обеспечение, но только 29% бюджетов корпоративной безопасности направлены на устранение данного типа уязвимостей.

Это показало исследование по инвестициям в безопасность встроенного ПО, проведенное компанией Security Signals в партнерстве с Microsoft. «Есть два вида организаций – те, кто подверглись атаке на микропрограммное обеспечение, и те, кто подвергся атаке на микропрограммное обеспечение, но пока не знают об этом», – отметил Азим Шафкат, бывший управляющий вице-президент Gartner.

Подавляющее большинство (82%) респондентов Security Signals сообщили, что у них нет ресурсов, которые можно было бы направить на более эффективную работу по обеспечению безопасности, поскольку они тратят слишком много времени на низкоуровневую ручную работу, такую как обновление программного и аппаратного обеспечения, тестирование патчей безопасности, а также аудит и устранение внутренних и внешних уязвимостей. 21% специалистов признают, что данные их прошивок остаются сегодня без контроля и защиты.

Согласно исследованию, текущие инвестиции идут на обновление системы безопасности, обнаружение уязвимостей и усовершенствование решений для защиты от угроз. Однако многие организации остаются обеспокоенными тем, что вредоносные программы позволяют получать доступ к корпоративным системам, а также трудностями в обнаружении угроз, что говорит о сложности мониторинга и контроля микропрограммного обеспечения. Проблема также усугубляется недостаточной осведомленностью об угрозах и отсутствием автоматизации защиты:

Недостаточная осведомленность. Микропрограммное обеспечение становится приоритетной мишенью для хакеров, ведь в нем хранится конфиденциальная информация, такая как учетные данные и ключи шифрования. Недавно Национальный институт стандартизации и технологий (NIST) показал более чем пятикратное увеличение числа атак на встроенное микропрограммное обеспечение за последние четыре года. Тем не менее, исследование Security Signals показывает, что уровень осведомленности об этой угрозе отстает от других отраслей. Даже при таком всплеске числа атак на микропрограммы, исследование показывает, что по мнению большинства специалистов, отвечающих за вопросы информационной безопасности, уязвимости в ПО в три раза чаще создают угрозу по сравнению уязвимостями в микропрограммах.

Проблема автоматизации. Отсутствие автоматизации является еще одним фактором, который вынуждает организации терять время и отвлекает их от разработки более эффективных стратегий превентивной защиты. 71% опрошенных специалистов утверждают, что их сотрудники тратят слишком много времени на работу, которая может и должна быть автоматизирована. В целом команды специалистов по ИБ тратят 41% своего времени на обновление микропрограмм.

Исследование Security Signals определило ядро ОС как растущую брешь в построении информационной защиты предприятия. Результаты также

свидетельствуют о том, что инвестиции в эту область остаются на низком уровне. Лишь 36% компаний инвестируют в аппаратное шифрование памяти ядра ОС, а менее половины (46%) – в аппаратную защиту ядра. Также Security Signals выявило, что команды безопасности слишком сфокусированы на устаревших моделях «защитить - обнаружить» и не тратят достаточно времени на разработку стратегии – только 39% времени команд безопасности тратится на профилактику, и, вероятно, это не изменится в ближайшие два года. Результатом такой устаревшей модели является отсутствие проактивных инвестиций в защиту от атак на ядро.

В SANS отмечают, что микропрограммное обеспечение управляет аппаратным оборудованием, но нет способа убедиться, что оно на 100% защищено. Атаки на микропрограммное обеспечение менее распространены, чем на программное обеспечение, но успешная атака будет намного более разрушительной.

Самым главным выводом из доклада Security Signals является то, что компании хотят иметь более проактивные стратегии в области безопасности, особенно когда речь идет о борьбе с атаками на микропрограммное обеспечение. Для удовлетворения этих потребностей компания Microsoft совместно с партнерами создала новый класс устройств, специально предназначенных для устранения угроз, направленных на микропрограммное обеспечение, под названием Secured-core PC. Они обеспечивают комплексную защиту электропитания с такими возможностями, как Virtualization-Based Security, Credential Guard и Kernel Direct Memory Access (DMA). Благодаря доступным «из коробки» возможностям и последующей автоматизации компании смогут освободить время, затрачиваемое на низкоуровневую деятельность, и направить свои усилия на осуществление коммерческих и стратегических задач». ***(Количество атак на микропрограммное обеспечение растет // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5728777-Kolichestvo-atak-na-mikroprogrammno.html). 13.04.2021).***

***

«Наконец-то из цифрового мира приходят хорошие новости: отчеты компании по культуре безопасности KnowBe4 показывают, что пользователи лучше распознают фишинговые атаки. Многие пользователи сообщают о попытках фишинга по электронной почте в соответствующие ИТ-отделы. Но с учетом сказанного, электронные письма - не единственное место, где происходит мошенничество. Теперь он также распространяется в социальных сетях, особенно в LinkedIn, по словам пользователей.

Раскрывая результаты отчетов, Стю Шоуверман, генеральный директор KnowBe4, сказал, что плохие парни по-прежнему продолжают то, что они делали в первом квартале. Но на этот раз только треть пользователей попалась на фишинговое письмо и перешла по ссылке, предлагающей проверить пароль. Сейчас все больше и больше пользователей проверяют свой ИТ-отдел, прежде чем доверять номеру телефона, адресу электронной почты или внутренней системе, поскольку они знают, что достаточно одного щелчка мыши, чтобы нанести ущерб.

Самые популярные фишинговые рассылки по электронной почте

Отчет KnowBe4 также включал список из 10 основных тем электронной почты, связанных с фишингом, которые пользователи получили и сообщили своим ИТ-отделам. Один взгляд на них показал, что некоторые из них казались настоящими фишинговыми атаками, тогда как другие были упражнениями моделирования фишинга.

Тема «Требуется немедленная проверка пароля» оказалась самой распространенной в электронных письмах - 31% жалоб. Этот термин чаще используется в симуляциях, но для реальных атак злоумышленники вносят изменения, чтобы повторно пройти аутентификацию ради доступа к электронной почте.

Другая атака, основанная на взломе паролей, гласила: «Google: примите меры для защиты своих скомпрометированных паролей».

Были также темы, такие как «HR: необходимо обновить данные о вашей заработной плате». а некоторые мошенники придумали слоганы с выигранными призами, кредитными картами, отклоненными Amazon Prime, пропущенными собраниями Zoom и сообщениями в профилях Facebook.

В каждом случае есть одна общая черта: войдите в систему, чтобы увидеть дополнительную информацию по этому вопросу.

Что случилось в социальных сетях?

Наряду с электронной почтой, социальные сети также стали горячей точкой для киберпреступников. В прошлом году LinkedIn неожиданно оказался лидером среди платформ, на которых было совершено большинство фишинговых атак, 42% электронных писем были связаны с ним.

В настоящее время также действуют активные кампании, нацеленные на пользователей LinkedIn. Об одном таком примере уже сообщал eSentire, согласно которому мошенники предлагают работу в LinkedIn с миссией установить бэкдоры с большим количеством яиц на компьютеры целевого пользователя.

Электронные атаки, основанные на LinkedIn, также заманивают жертв, обещая им хорошее появление в поиске, новые подключения или сброс пароля при необходимости. Хуже всего то, что люди попадают на это, щелкая ссылку, упомянутую в фишинговых письмах.

20% атак также выполнялись в виде тегов к фотографиям на Facebook, тогда как оповещения о входе в Chrome на Moto X неожиданно заняли третье место с 12% атак, использующих эту стратегию.

Конечный результат

Несмотря на то, что пользователи начинают умнее выявлять такие мошенничества, это не помешает злоумышленникам пробовать новые способы с помощью фишинговых писем.

Итак, все, что вам нужно сделать, это всякий раз, когда вы подозреваете, что ссылка не является законной, всегда подтверждайте, прежде чем нажимать на любую ссылку, упомянутую в электронных письмах. Эти ссылки всегда приводят вас на фиктивный сайт, где они пытаются украсть вашу личную информацию.

Получив подробную информацию, киберпреступники изменяют ваши пароли в экземпляре, заменяют ваш номер телефона своим, а также меняют ваш адрес

электронной почты. В результате вы теряете полный доступ к своей учетной записи.

Если вы получили электронное письмо с предупреждением об изменении пароля для любого сайта социальной сети, убедитесь, что вы посетили соответствующую платформу социальных сетей, чтобы действительно подтвердить, требуется ли сброс пароля или это поддельное письмо, которое вы получили.

То же действие будет применяться к рабочим сайтам или сайтам электронной коммерции, и рекомендуется, чтобы пользователи обычно входили в систему на платформе, прежде чем делать какие-либо действия». ***(Daniyal Malik. Finally, Reports Show That Users Are Getting Better At Identifying and Dealing With Phishing Scams // Digital Information World (https://www.digitalinformationworld.com/2021/04/finally-reports-show-that-users-are.html). 26.04.2021).***

***

«Удаленная работа, по крайней мере в той или иной форме, никуда не денется. Технологические гиганты, такие как Facebook, Shopify и Twitter, и многие другие заявили, что позволят сотрудникам работать из дома, даже если возвращение в офис считается безопасным.

Эти шаги становятся популярными, и многие сотрудники приветствуют эту идею и хотели бы продолжить работу из дома. Действительно, в новой гибридной модели работы есть много положительных моментов как для сотрудников, так и для предприятий, например, сокращение количества поездок на работу и возможность для организаций нанимать более широкую базу кандидатов без географических ограничений.

Но есть и обратные стороны. Одна из фундаментальных проблем, связанных с удаленной и гибридной работой, связана с кибербезопасностью, поскольку некоторые сотрудники могут с большей вероятностью пойти на кибер-риски дома, чем в офисе. Эти изменения могут сделать компании уязвимыми для рисков кибербезопасности и соблюдения нормативных требований, а кибератака может иметь огромные финансовые и бизнес-последствия для организации.

Поскольку удаленная работа является частью «следующей нормы», как сейчас, так и в будущем, компаниям необходимо уделять приоритетное внимание кибербезопасности удаленных сотрудников. Многие компании уже установили подключение и удаленные рабочие процессы для достижения бизнес-целей за последний год; теперь требуется оценить безопасность и убедиться, что они не представляют собой легких целей для киберпреступников.

Последствия кибератак

Опрос Malwarebytes показал, что с начала пандемии нарушения безопасности у ошеломляющих 20% респондентов были результатом удаленных сотрудников. Кибератаки могут иметь пагубные последствия для всей организации, и их предотвращение должно быть приоритетной задачей бизнеса.

Наиболее очевидные последствия невыполнения этого требования - финансовые, особенно если кибербезопасность связана с мошенническими

банковскими переводами. Однако их влияние может быть гораздо глубже. Даже если деньги напрямую не задействованы, атака все равно может иметь негативные фискальные последствия для прибыли бизнеса. Существуют затраты на реагирование и восстановление, затраты на расследование, сложность упущенного дохода, а также затраты на юридические услуги и связи с общественностью, и это лишь некоторые из них.

Я видел, что кибератака также может привести к снижению производительности. Медленные технологии или простои технологий означают, что сотрудники не могут получить доступ к критически важным для бизнеса приложениям и системам. Снижение производительности и увеличение затрат, которые возникают в результате, могут подорвать текущую непрерывность бизнеса и даже остановить рост бизнеса в будущем.

Незащищенный персонал также ставит под угрозу критически важные данные о клиентах. Потребители и предприятия хотят взаимодействовать с организациями, которые бережно и безопасно обрабатывают их данные. В прошлом году произошли серьезные взломы с участием Twitter, Zoom и нескольких организаций здравоохранения. Учитывая важную роль Zoom в поддержании работы бизнеса во время пандемии, его взлом и потеря в апреле 2020 года 500000 паролей клиентов могут ощущаться во всей бизнес-экосистеме.

Доверие здесь является жизненно важным компонентом. В то время как утечки данных в настоящее время имеют реальные последствия для организаций в соответствии с положениями Общего регламента по защите данных и другого соответствующего законодательства во всем мире, доверие и его потерю труднее точно измерить. Потеря доверия клиентов пагубно сказывается на репутации бренда, и вернуть ее может быть непросто.

Принятие целостного подхода

Комплексная защита персонала, включая людей, которые ежедневно работают с клиентами и их данными, может защитить компании от долгосрочного ущерба репутации.

Обеспечение безопасности гибридных сотрудников, где бы они ни находились, теперь является важным компонентом обеспечения будущего успеха в бизнесе. Компаниям следует стремиться к развертыванию целостной стратегии безопасности, которая не только включает продукты и услуги, но и использует опыт своих специалистов по безопасности и признает, что безопасность - это непрерывный процесс. Точно так же, как киберпреступники никогда не перестанут развивать свои методы атак, инструменты, препятствующие их успеху, также должны постоянно развиваться.

Используя целостный подход, вы можете разработать, внедрить и поддерживать эффективную систему безопасности, которая включает в себя всю ИТ-инфраструктуру и использует существующие технологии.

Целостная стратегия безопасности должна быть гибкой, адаптируемой и простой в управлении. Шаги по созданию комплексного подхода к безопасности различаются в зависимости от потребностей компании, но должны включать:

• Определение рисков в вашей организации: понимание вашей уязвимости к атакам имеет решающее значение для принятия правильной структуры.

• Создание спроектированной, тесно интегрированной экосистемы: многие из них сегодня можно автоматизировать для борьбы с атакой до того, как она произойдет.

• Распознавание атак. Знание различных стадий атаки программы-вымогателя поможет вам определить, как лучше всего защитить вашу компанию.

• Согласование стратегии безопасности с операциями: для хорошо построенной стратегии безопасности координация с бизнес-операциями важна для защиты нужных активов и обеспечения безопасности бизнеса в будущем.

• Масштабирование для будущего: используйте управляемые услуги для непрерывного масштабного внедрения инноваций.

Без надежной рабочей силы компании могут нанести долгосрочный ущерб своему бизнесу. Тем не менее, имея надежную рабочую силу, вы получаете выгоду от страхования от повреждений и потерь и предлагает более безопасное и надежное обслуживание своим клиентам и сотрудникам». ***(Robert Bailkoski. Why Cybersecurity Needs To Be A Top Priority For The C-Suite Today // Forbes (https://www.forbes.com/sites/forbesbusinesscouncil/2021/04/30/why-cybersecurity-needs-to-be-a-top-priority-for-the-c-suite-today/?sh=7254bcc71c39). 30.04.2021).***

***

«Пандемия Covid-19 продемонстрировала городам всего мира важность программ умного города с использованием технологий, данных и инновационных решений для решения их социальных, экологических и экономических проблем.

Действительно, 65 процентов руководителей городов, опрошенных в 2020 году в рамках проекта ESI ThoughtLab's Smart City Solutions for a Risker World, сообщили, что главные уроки, извлеченные из пандемии, заключаются в том, что программы умного города имеют решающее значение для их будущего.

Подверженность риску

Однако инновации - это палка о двух концах. По мере того, как руководители городов увеличивают свои инвестиции в цифровые технологии, они также подвергают свои города повышенным рискам кибербезопасности, если не принимают соответствующие меры безопасности заранее.

Пандемия стала стресс-тестом для городских систем кибербезопасности. Количество атак на правительства штатов и местных властей резко возросло, поскольку киберпреступники пытались воспользоваться кризисом.

Многие города стали жертвами программ-вымогателей и других векторов атак. Например, Ноксвилл в Теннесси в июне 2020 года подвергся атаке, которая нанесла ущерб его ИТ-системам. Сбои обострились, когда хакеры начали публиковать данные в Интернете, чтобы получить выкуп. Хакеры также воспользовались беспорядком, связанным с пандемией, и бесстыдно атаковали некоторые больницы.

Исследование ESI ThoughtLab показывает, что городам необходимо делать больше для обеспечения безопасности своих городских центров и жителей. Большинство городов (60 процентов) сообщили, что они плохо подготовлены к кибератакам. Хотя малые города были более уверены в своих системах

кибербезопасности, чем другие, самые маленькие городские районы находятся в более опасной ситуации, и только 29 процентов считают, что они хорошо подготовлены. Это подтверждается частотой атак во время пандемии в небольших городах США, таких как Флоренция, Алабама и Пенсакола, Флорида.

Одним из признаков лидера умного города, наиболее продвинутого в использовании технологий и инновационных решений, является его уровень кибербезопасности. Девяносто пять процентов городов, признанных лидерами в исследовании, заявили, что они хорошо подготовлены к кибератакам, по сравнению с 8 процентами. цент начинающих городов.

Лучшие практики кибербезопасности

Есть передовые методы, которым города могут следовать, чтобы укрепить свою защиту от нападений. Городским менеджерам следует взять лист из сборника уроков руководителей умного города.

Есть пять ключевых шагов кибербезопасности, которые лидеры предпринимают гораздо чаще, чем другие города, для устранения своих уязвимостей кибербезопасности:

Расставьте приоритеты для активов и создайте политики контроля доступа. Защита наиболее ценных активов города - это первый разумный шаг, так же как и обеспечение строгого контроля в городе над тем, кто может получить доступ к его системам.

Инвестируйте в технологии аварийного восстановления, реагирования и управления событиями. Независимо от того, насколько сильны городские брандмауэры, достаточно одного плохого парня, чтобы пройти. Поэтому лидеры умных городов вкладывают больше средств в специализированные технологии восстановления и реагирования, чтобы действовать быстро и смягчать последствия.

Проведите обучение персонала по вопросам кибербезопасности. Это критически важный шаг для городов, поскольку киберпреступники часто извлекают выгоду из ошибок сотрудников.

Защитите критически важную инфраструктуру. Это включает тестирование безопасности электрических сетей, светофоров, больниц и других городских объектов. Соединение городских активов и доменов с помощью Интернета вещей и других технологий может подвергнуть города катастрофической атаке, если они не обеспечат надлежащую защиту своей инфраструктуры.

Разработайте план реагирования на киберинциденты и восстановления. Руководители умных городов понимают, что им нужно не только действовать быстро, чтобы остановить атаку, но и иметь процессы, ограничивающие последствия, в том числе связанные с ответственностью, финансовым и репутационным воздействием.

Уроки кибератаки

Одним из небольших городов, который осознал ценность таких передовых методов, был Торранс, штат Калифорния. 1 марта 2020 года в Торрансе произошел киберинцидент, который отрицательно повлиял на работу города. Всего две недели спустя Торранс объявил местное чрезвычайное положение из-за пандемии коронавируса.

Столкнувшись с двумя серьезными кризисами, руководители города попытались создать виртуальный центр аварийных операций (EOC) через Slack, облачную платформу обмена сообщениями, размещенную на Amazon Web Services. Город использовал Google Диск для всех своих форм и документов вместо электронной почты, поскольку это было безопаснее и эффективнее.

В течение недели город перешел от кирпича и раствора, бумаги и карандаша к виртуальным операциям. Затем он смог подключить районные больницы, местный школьный округ, Красный Крест, Армию спасения и бизнес-группы к EOC для обмена информацией в режиме реального времени. А когда несколько месяцев спустя Торранс и Южная Калифорния испытали гражданские беспорядки - еще одно потрясение, - Slack позволил городу сгладить информационную кривую и поделиться данными внутри и конфиденциально для повышения осведомленности о событиях.

Городские власти смогли направить живые изображения событий прямо в Slack, где каждый, кто участвовал в управлении реагированием, мог видеть и лучше понимать ситуацию. «Больше не было разрозненности, которая могла образоваться, потому что все департаменты были распущены», - сказал Джеффри Снодди, менеджер службы экстренной помощи города.

Этот опыт стал откровением, и с тех пор город разработал план кибербезопасности. Персоналу рассылаются напоминания о методах обеспечения безопасности, например, о регулярной смене паролей и подключении из дома только к устройствам, выпущенным в городе. Город также проводит рутинную оценку степени риска своих уязвимых мест.

«Устойчивость и ловкость необходимы для выживания и процветания», - сказал городской менеджер Торранса Арам Чапарян. «Правительства действуют более медленными темпами, потому что мы несем фидуциарную ответственность. Мы осуществляем надзор со стороны избранных нами должностных лиц и общественности. У нас нет роскоши времени. Это не если, это когда у нас будет еще один кризис, и все дело в создании состояния готовности». ***(Cybersecurity: a smart city imperative // SmartCitiesWorld (https://www.smartcitiesworld.net/special-reports/cybersecurity-a-smart-city-imperative). 30.04.2021).***

***

«В 2020 году Cisco обнаружила, что 50% крупных предприятий (с более чем 10 000 сотрудников) тратят 1 миллион долларов и более в год на безопасность, при этом 43% тратят от 250 000 до 999 999 долларов и только 7% тратят менее 250 000 долларов.

Согласно новому отчету PMMI Business Intelligence «Кибербезопасность 2021: оцените свой риск», для этих производителей опасности кибератаки вполне реальны, и может быть сложно идти в ногу с быстрыми темпами развития кибербезопасности. Хотя производителям легко почувствовать себя беспомощными перед изощренными технологическими атаками, существуют четко определенные шаги для защиты операционной безопасности, первая из которых - это всесторонний подробный анализ операционных уязвимостей.

Как только производители поймут, что это за операционные уязвимости и где они расположены, они могут приступить к защите сетей, а также установить и применять передовые методы кибербезопасности в своих местах. Один управляющий директор одного из киберпартнеров сказал: «Оценка риска является ключом к установлению базовых показателей того, где находятся ваши уязвимости сегодня, какие важные данные собираются и как эти данные защищаются».

Комплексная оценка включает:

• Производители сначала должны иметь полное представление о том, каковы их собственные операционные уязвимости и где они существуют в их организации.

• Производители должны проводить тщательную оценку своих систем, устройств, оборудования, сетей и всех других точек подключения как внутри, так и за пределами своей деятельности.

• Производители должны понимать структуру своих внутренних сетей: как отдельные компоненты (включая устройства сотрудников, такие как телефоны) подключены друг к другу, как отдельные сети связаны друг с другом, как / если разрешен удаленный доступ, и где любой внешний возможность подключения (например, подключение к Интернету) постоянно.

Учитывая увеличение частоты атак на основе ОТ, организациям особенно важно иметь подробное представление об архитектуре АСУ ТП. Также необходимо получить исчерпывающее представление о потоке данных: как собираются данные, где они хранятся и кто имеет к ним доступ - это также включает все возможности периферийных вычислений и облачных вычислений.

Далее - Выделенная команда:

После того, как составлен исчерпывающий и подробный обзор операций и уязвимостей организации, производители должны перейти к активному отслеживанию любой подозрительной активности. Производители должны серьезно рассмотреть возможность размещения специальной группы, оснащенной надежным набором программного обеспечения, предназначенного для мониторинга и выявления любой подозрительной деятельности, отвечающей за наблюдение за сетевой активностью организации. Компании сообщают, что бремя защиты от кибератак в последние годы возросло, при этом 58% заявили, что обнаружение угроз и реагирование на них постоянно усложняются. Эта борьба имеет смысл: поскольку в последние годы частота кибератак резко возросла, по оценкам одного из анализов, каждую минуту киберпреступность теряет 2,9 миллиона долларов.

Информация о безопасности и управление событиями (SIEM):

Платформа SIEM является неотъемлемой частью мониторинга кибербезопасности, предоставляя производителям подробное представление о своем сетевом трафике. Хотя все системы незначительно различаются и существует множество поставщиков, SIEM часто может выполнять такие функции, как:

• Агрегация данных для управления журналами

• Корреляция данных для представления информации в удобной форме

• Проактивные оповещения, созданные на основе автоматического анализа событий, которые могут отображаться в режиме реального времени на информационной панели.

Организация данных:

Производители должны гарантировать, что их эксперты по кибербезопасности должным образом наделены данными, которые им необходимы для эффективной защиты организации. Данные и статистика по сетевому трафику и частоте входа в систему бесполезны, если группа, отвечающая за кибербезопасность, не может легко найти, получить доступ и использовать их по запросу в работоспособном формате.

Самое главное - бдительное тестирование:

Прежде всего, для того, чтобы любая стратегия кибербезопасности была эффективной в долгосрочной перспективе, необходима бдительность. Любые изменения или корректировки оборудования, программного обеспечения, графиков производства, сбора данных, отчетности, персонала и физической инфраструктуры предприятия влекут за собой многочисленные соображения по обеспечению кибербезопасности.

Надежный план кибербезопасности требует постоянного обновления и корректировки по мере появления новых факторов в процессах организации. По этой причине производителям выгодно периодически проверять свою кибербезопасность, выполняя имитацию атак для проверки реакции; обеспечение своевременности планов кибербезопасности и одновременное поддержание готовности их команды кибербезопасности.

Проблемы:

80% опрошенных компаний заявили, что они понятия не имеют, где в их организации находятся конфиденциальные данные, и не знают, были ли они в безопасности.

Опрошенные производители брендов перечисляют препятствия на пути к обеспечению более безопасной работы, такие как непонимание рисков кибератак, устаревшее оборудование и программное обеспечение, адекватный бюджет, нехватка персонала, невнимательность сотрудников и формирование культуры «безопасность прежде всего». ***(Kim Overstreet. The First Step to Increasing Cybersecurity // PMMI Media Group (https://www.packworld.com/home/article/21403576/the-first-step-to-increasing-cybersecurity-is-to-analyze-operational-vulnerabilities). 27.04.2021).***

***

«Большинство предприятий в качестве стандартной практики проводят регулярную оценку рисков. Они имеют решающее значение для снижения угрозы финансовых или репутационных потерь и дают вам обзор областей повышенного риска, которые вы должны решить.

Один из видов анализа рисков, который имеет решающее значение, но иногда упускается из виду, - это оценка рисков кибербезопасности. В современном мире цифровых технологий трудно переоценить важность анализа и устранения угроз вашей ИТ-безопасности. Что делает его обычное явление, также рекомендуется,

потому что киберпреступники будут находить новые дыры в вашей обороне каждый день.

Для устранения этих угроз необходимы полные и частые аудиты кибербезопасности для проверки:

Слабые места в ваших бизнес-системах.

Устаревшее оборудование или программное обеспечение.

Осведомленность ваших сотрудников о безопасности.

Вот основные шаги, которые необходимо предпринять для проведения оценки рисков кибербезопасности.

Проведите аудит вашего оборудования и бизнес-систем

Вы не сможете понять риски, связанные с вашей технологией, если не будете отслеживать ее в первую очередь. Вести полный учет всех технологий в вашем бизнесе иногда бывает непросто. Если отделы вашего бизнеса делают теневые закупки ИТ - внедряют технологию без одобрения ИТ-команды - это может быстро стать неуправляемым.

Выявление и аудит ваших наиболее важных и широко используемых ИТ-активов поможет вам понять, какие решения составляют наибольший процент поверхности для ваших атак. Например, большинство ваших сотрудников, скорее всего, будут использовать ваше программное обеспечение для управления взаимоотношениями с клиентами (CRM). Если вы не ограничили права доступа, хакеры могут проникнуть через бэкдор. Точно так же вы можете запретить людям обмениваться информацией о клиентах извне, ограничив количество людей, которые могут загружать большие объемы данных.

Наличие постоянно обновляемого комплекта вашего оборудования также позволит вам запланировать установку исправлений. Обновление хорошо известных угроз безопасности, таких как неподдерживаемые устройства или операционные системы (ОС), должно иметь высокий приоритет. Windows 7, срок жизни которой подошел к концу в январе 2020 года, подверглась мошенничеству с кражей паролей из-за ее уязвимостей. Это подчеркивает важность регулярного исправления программного и аппаратного обеспечения.

Рассмотрите наиболее вероятные инциденты

Когда мы думаем об усилении нашей кибербезопасности, естественно сосредоточиться на защите вашего бизнеса от внешних угроз, таких как хакеры. Это важно, но вам также необходимо посмотреть на другие распространенные инциденты и их риски.

В силу вступления в силу GDPR безопасность данных является одним из приоритетов для большинства предприятий. Важно отметить, что бизнес-данные могут быть скомпрометированы как случайно, так и намеренно. Если ваши люди используют съемные устройства хранения данных, такие как USB-накопители, есть риск их потери или кражи - как в случае с аэропортом Хитроу.

Точно так же, если киберпреступники нацелены на ваш бизнес с помощью фишинговых писем, примите во внимание уровень риска, который ваши люди будут нажимать на вредоносные ссылки и заполнять свои данные для входа. Вы можете снизить вероятность того, что эти угрозы достигнут ваших сотрудников, в первую очередь, используя мощные инструменты фильтрации электронной почты.

Поскольку инструменты хакеров, такие как высокоразвитая программа-вымогатель Ryuk, постоянно становятся все более изощренными, вам необходимо подумать о том, что будет дальше.

Информирование ваших сотрудников о ландшафте киберугроз и о том, как они могут сыграть роль в обеспечении безопасности вашего бизнеса, имеет жизненно важное значение. Вы можете сделать это:

Предоставление цифровых и очных учебных материалов.

Использование инструмента моделирования фишинга для проверки имеющихся знаний персонала.

Аутсорсинг обучения безопасности для управляемой ИТ-поддержки.

Определите уровень риска и расставьте приоритеты в действиях

Оценка рисков не заканчивается после того, как вы определили наиболее значимые риски. Затем вам необходимо понять, как бороться с выявленными вами рисками.

Допустим, вы знаете, что многие ваши сотрудники берут конфиденциальную информацию на встречи с клиентами на месте с помощью USB-накопителей. Они путешествуют на общественном транспорте, и их устройства хранения не зашифрованы. Это означает, что ваша уязвимость высока: существует высокий риск потери или кражи этих предметов и доступа к ним злоумышленников.

Поэтому это должно быть одним из первых вопросов, к которым вы обращаетесь. Вы можете разделить действия на быстрые победы и долгосрочные стратегии. Таким образом, быстрой победой будет реализация политики, согласно которой съемные устройства хранения данных должны быть зашифрованы и / или защищены паролем. Долгосрочная стратегия может заключаться в реализации решения для облачного хранилища, которое позволит вашим сотрудникам получать доступ к своим документам в любое время и в любом месте и устранить необходимость в USB-накопителях.

Не забывайте о своей удаленной рабочей силе

Если в вашем бизнесе есть сотрудники бэк-офиса, скорее всего, часть из них в настоящий момент будет работать из дома. Фактически, согласно опросу бизнес-школы IESE, SD Worx и CASS Business School, 65% всех британских сотрудников перешли на удаленную работу во время блокировки.

Это создает дополнительные риски для безопасности вашего бизнеса.

Исследование, проведенное IBM, показало, что 53% удаленных сотрудников работают со своими личными устройствами, а 61% заявили, что их работодатель не выпустил никаких инструкций по обеспечению безопасности этих устройств. Это представляет ряд рисков для вашей безопасности, в том числе:

Решения низкого уровня безопасности на личных устройствах ваших сотрудников, оставляющие бреши для хакеров

Скрытое вредоносное или вредоносное ПО, которое было установлено по незнанию

Конфиденциальная информация доступна для лиц, не являющихся сотрудниками.

Вы можете легко снизить эти риски, предоставив сотрудникам ноутбуки или, если это невозможно, облачные хранилища корпоративного уровня, которые

добавляют уровни защиты к рабочим файлам. Точно так же незащищенные домашние сети Wi-Fi представляют опасность для безопасности. Установив бизнес-виртуальную частную сеть (VPN), вы можете зашифровать подключение сотрудников к вашей сети.

В наш информационный век оценка рисков кибербезопасности является неотъемлемой частью бизнес-процессов. Хакеры прямо сейчас пользуются преимуществами бизнеса и своих надомников, что означает увеличение вашей поверхности атаки. Проведя тщательную оценку рисков, вы сможете определить системы, которые в первую очередь нуждаются в защите. Затем вы можете создать комплексный план действий, который в первую очередь касается областей вашего бизнеса с высоким уровнем риска, прежде чем приступить к защите каждой потенциальной точки входа для киберпреступников». ***(Barry O'Donnell. Creating a cybersecurity risk assessment // Open Access Government (https://www.openaccessgovernment.org/creating-a-cybersecurity-risk-assessment/109270/). 27.04.2021).***

***

Сполучені Штати Америки

«В рамках своих усилий по защите активов пенсионных планов на сумму около 9,3 триллиона долларов от растущих «внутренних и внешних угроз кибербезопасности» Министерство труда (DOL) выпустило первое руководство в отношении кибербезопасности и пенсионных планов. Руководство предназначено для трех заинтересованных групп, заинтересованных в администрировании пенсионных планов: спонсоров и доверенных лиц пенсионных планов; организации, предоставляющие административные и другие услуги пенсионным планам; и планируйте участников и бенефициаров.

Новые «Советы по онлайн-безопасности» DOL для участников и бенефициаров плана предлагают удобное для пользователя краткое изложение того, какие шаги следует предпринять в любом случае для защиты своей личной финансовой и другой информации от угроз сетевой безопасности. Но спонсоры плана и доверенные лица должны уделять особое внимание «Передовой практике программы кибербезопасности» и «Советам по найму поставщика услуг с надежной практикой кибербезопасности» и соответствующим образом изменять свои текущие административные методы.

Указатель практики: спонсоры и доверенные лица плана должны ожидать, что это новое руководство послужит основой для будущих аудитов пенсионных планов DOL и скорректирует свои программы безопасности в соответствии с передовыми практиками DOL. Действительно, некоторые планы уже рассматривают эту проблему как компонент случайных аудитов планов DOL.

Лучшие практики программы кибербезопасности

DOL сообщает, что он подготовил свои передовые методы программы кибербезопасности для использования регистраторами и другими поставщиками плановых услуг, ответственными за защиту данных пенсионных планов и для

оказания помощи спонсорам плана в принятии разумных решений при выборе поставщиков плановых услуг. Это далеко идущее руководство сосредоточено вокруг 12 практик, которые спонсоры и доверенные лица должны ожидать от своих поставщиков плановых услуг:

Иметь официальную, хорошо задокументированную программу кибербезопасности.

Ежегодно проводите осмотрительную оценку рисков.

Проводите надежный ежегодный сторонний аудит средств безопасности.

Четко определите и распределите роли и обязанности в области информационной безопасности.

Используйте строгие процедуры контроля доступа.

Убедитесь, что любые активы или данные, хранящиеся в облаке или управляемые сторонним поставщиком услуг, подлежат соответствующему анализу безопасности и независимой оценке безопасности.

Проводите периодические тренинги по повышению осведомленности о кибербезопасности.

Внедрение и управление программой жизненного цикла разработки безопасной системы (SDLC).

Разработайте эффективную программу обеспечения устойчивости бизнеса, направленную на обеспечение непрерывности бизнеса, аварийного восстановления и реагирования на инциденты.

Шифруйте конфиденциальные данные, хранящиеся и пересылаемые.

Внедрите строгий технический контроль в соответствии с передовыми методами безопасности.

Надлежащим образом реагируйте на любые прошлые инциденты, связанные с кибербезопасностью.

Каждый из этих элементов более подробно описан в руководстве, в частности, лучшие компоненты надежного набора письменных политик и процедур безопасности для реализации этих рекомендуемых шагов. Если возможно, спонсор плана и доверенные лица должны запросить подтверждение такой письменной программы передового опыта и сохранить его вместе с файлами плана.

Советы по найму поставщика услуг с надежной практикой кибербезопасности

Новые советы DOL по найму поставщика услуг с надежной практикой кибербезопасности аналогичным образом прослеживают для лиц, принимающих решения по плану, элементы разумного процесса выбора и мониторинга поставщиков услуг пенсионного плана. Спонсоры и доверенные лица плана должны быть готовы:

Спросите о стандартах, методах и политиках информационной безопасности поставщика услуг, а также о результатах аудита и сравните их с отраслевыми стандартами, принятыми другими финансовыми учреждениями.

Спросите поставщика услуг, как он проверяет свои методы, какие уровни стандартов безопасности он соблюдал и внедрял, а также о праве проверять результаты аудита, демонстрирующие соответствие стандарту.

Оцените послужной список поставщика услуг в отрасли, включая общедоступную информацию об инцидентах информационной безопасности, других судебных разбирательствах и судебных разбирательствах, связанных с услугами поставщика.

Спросите, сталкивался ли поставщик услуг с нарушениями безопасности в прошлом, что произошло и как поставщик услуг отреагировал.

Узнайте, есть ли у поставщика услуг какие-либо страховые полисы, покрывающие убытки, вызванные нарушениями кибербезопасности и кражи личных данных (включая нарушения, вызванные внутренними угрозами, такими как неправомерные действия собственных сотрудников или подрядчиков поставщика услуг, а также нарушения, вызванные внешними угрозами, такими как третье лицо захватывает аккаунт участника плана).

Убедитесь, что договор с поставщиком услуг требует постоянного соблюдения стандартов кибербезопасности и информационной безопасности, и избегайте положений договора, которые ограничивают ответственность поставщика услуг за нарушения безопасности.

Кроме того, контракты должны включать условия, которые улучшат защиту кибербезопасности для плана и его участников, такие как отчетность по информационной безопасности, четкие положения об использовании и обмене информацией и конфиденциальности, уведомление о нарушениях кибербезопасности, соблюдение требований к хранению и уничтожению записей, конфиденциальность. законы об информационной безопасности и страхование.

Указатель практики: особенно важно отметить выше условия, касающиеся вопросов кибербезопасности, которые DOL ожидает увидеть в контрактах с поставщиками плановых услуг. Спонсорам плана и фидуциарам рекомендуется следовать процессу, описанному в Совете по найму поставщика услуг с надежной практикой кибербезопасности, и быть готовыми задокументировать - и подготовить такую документацию после аудита - шаги, предпринятые при выборе и мониторинге поставщиков услуг плана.

По мере того, как онлайн-угрозы безопасности личной информации становятся все более и более распространенными, для спонсоров и доверенных лиц плана как никогда важно поддерживать ответственные и осмотрительные методы защиты информации об учетных записях участников и бенефициаров пенсионных планов. Новое руководство DOL возлагает ответственность непосредственно на спонсоров и доверенных лиц плана, а также на поставщиков услуг, которых они привлекают для привлечения внимания к этим важным вопросам, и предоставляет своего рода дорожную карту для облегчения внедрения передовых методов кибербезопасности. Планы также должны ожидать увеличения активности аудита DOL в отношении планов кибербезопасности…» ***(ANDREW ELBON. Cybersecurity: New DOL Guidance for Retirement Plans // BRADLEY ARANT BOULT CUMMINGS LLP (https://www.bradley.com/insights/publications/2021/04/cybersecurity-new-dol-guidance-for-retirement-plans). 16.04.2021).***

***

«Ранее в этом месяце, в ответ на недавний федеральный отчет, содержащий рекомендации по устранению рисков кибербезопасности для пенсионных планов, данных об участниках плана и активов плана, отдел администрирования безопасности льгот сотрудникам DOL (EBSA) опубликовал руководство по кибербезопасности для покрываемых ERISA пенсионные планы. В руководстве рассматриваются передовые практики для поставщиков плановых услуг, поскольку в нем содержатся советы как спонсорам плана, так и участникам плана. В руководстве конкретно упоминается пенсия и пенсия, и это относится ко всем планам, которые регулируются ERISA. Соответственно, планы медицинского страхования и социального обеспечения, регулируемые ERISA, также должны соответствовать рекомендациям EBSA.

Планы, управляемые ERISA, все чаще становятся объектами киберугроз из-за количества активов плана, принадлежащих одному плану. В этом руководстве подчеркивается, что DOL считает, что планы должны быть защищены. Кроме того, суды недавно издали постановления, согласно которым данные участников плана могут считаться активом плана. Это означает, что доверительные управляющие должны проявлять осторожность, чтобы защитить данные участников, как если бы это были фактические средства плана.

Учитывая все более удаленную рабочую силу для многих спонсоров планов, это новое руководство особенно актуально. Если вы являетесь доверенным лицом плана и у вас нет политики кибербезопасности для своего плана, сейчас самое время это сделать. Если у вас уже есть политика кибербезопасности, сейчас самое время пересмотреть и обновить ее в свете этого нового руководства.

В руководстве EBSA указывает, что, по ее мнению, является «передовой практикой» для всех поставщиков услуг ERISA. Эти передовые практики предусматривают, что поставщик услуг должен делать следующее:

Разрабатывать, документировать, регулярно отслеживать и обновлять официальную программу кибербезопасности.

Проводите осмотрительную ежегодную оценку рисков

Ежегодно проводите надежный сторонний аудит средств контроля безопасности.

Четко определите и распределите роли и обязанности в области информационной безопасности

Иметь строгие процедуры контроля доступа

Убедитесь, что любые активы или данные, хранящиеся в облаке или управляемые сторонним поставщиком услуг, подлежат соответствующему анализу безопасности и независимой оценке безопасности.

Проводите регулярные тренинги по информационной безопасности.

Внедрить программу жизненного цикла разработки безопасной системы и управлять ею

Иметь эффективную программу обеспечения устойчивости бизнеса, направленную на обеспечение непрерывности бизнеса, аварийного восстановления и реагирования на инциденты.

Шифровать конфиденциальные данные, хранящиеся и передаваемые

Внедрите строгий технический контроль в соответствии с передовой практикой безопасности

Надлежащим образом реагируйте на любые прошлые инциденты, связанные с кибербезопасностью

Следуйте советам по найму поставщика услуг с надежными методами кибербезопасности.

Обучите участников принципам онлайн-безопасности.

Многие из приведенных выше рекомендаций очень похожи на те, которые содержатся в HIPAA для защиты данных о здоровье. Поскольку спонсоры плана оценивают своих поставщиков услуг и свои собственные внутренние методы работы, это руководство должно быть в центре внимания. В будущих RFP следует, как минимум, запрашивать информацию о двенадцати «лучших практиках» EBSA. DOL также заявил, что спонсоры плана должны учитывать это руководство при переговорах со своими поставщиками услуг. В будущих контрактах особое внимание должно уделяться совместному использованию и хранению информации и другим вопросам, о которых идет речь…». ***(John Kirk. If You Have An ERISA Plan, You Need To Think About Cybersecurity // Graydon Head & Ritchey LLP (https://graydon.law/if-you-have-an-erisa-plan-you-need-to-think-about-cybersecurity/). 27.04.2021).***

***

«12 апреля 2021 года администрация Байдена объявила о намерении назначить Криса Инглиса, бывшего заместителя директора Агентства национальной безопасности, первым национальным кибердиректором США («НИЗ») при условии утверждения Сенатом. Недавно созданная должность по НИЗ, которая будет выполнять функции главного советника президента по политике и стратегии в области кибербезопасности, и Управление национального директора по кибербезопасности («ONCD») были созданы в соответствии с Законом о государственной обороне на 2021 финансовый год («NDAA »), Который вступил в силу 1 января 2021 года.

ONCD создается при Администрации Президента. Помимо работы в качестве главного советника президента по политике и стратегии кибербезопасности, в обязанности НИЗ входит:

• предлагать советы и консультации Совету национальной безопасности, Совету внутренней безопасности и соответствующим федеральным департаментам и агентствам, связанным с разработкой и координацией национальной политики и стратегии в области киберпространства;

• координировать реализацию национальной киберполитики и стратегии;

• координировать разработку и обеспечивать реализацию комплексного реагирования федерального правительства на инциденты со значительными последствиями кибератак и кибер-кампаний;

• подготовить ответ федерального правительства на серьезные кибератаки и кибер-кампании в федеральных департаментах и агентствах, отвечающих за кибербезопасность, а также в соответствующих организациях частного сектора;

• координировать и консультироваться с лидерами частного сектора по вопросам кибербезопасности и новых технологий в поддержку и в координации с другими руководителями федеральных агентств и департаментов, такими как директор Агентства по кибербезопасности и безопасности инфраструктуры и директор национальной разведки;

• ежегодно отчитываться перед Конгрессом об угрозах кибербезопасности и проблемах, с которыми сталкиваются США, в том числе в отношении новых или появляющихся технологий, которые могут повлиять на национальную безопасность, экономическое процветание или обеспечение верховенства закона; а также

• нести ответственность за такие другие функции, которые может поручить Президент.

NCD уполномочен NDAA обнародовать правила и положения, которые могут быть необходимы для выполнения функций, полномочий и обязанностей, возложенных на NCD. Создание утвержденных Сенатом НИЗ и ONCD было рекомендациями отчета Комиссии по киберпространству по солярию от 2020 года, которой Конгресс поручил выработать консенсус в отношении стратегического подхода к защите США от кибератак со значительными последствиями». ***(White House to Nominate First National Cyber Director // Hunton Andrews Kurth LLP. (https://www.huntonprivacyblog.com/2021/04/14/white-house-to-nominate-first-national-cyber-director/#page=1). 14.04.2021).***

***

«14 апреля 2021 г. Управление безопасности выплат сотрудникам («EBSA») опубликовало руководство для спонсоров плана, доверенных лиц плана, регистраторов и участников плана по передовым методам обеспечения кибербезопасности. Это первый раз, когда EBSA дало рекомендации по кибербезопасности для 34 миллионов участников плана с установленными выплатами и 106 миллионов участников плана с установленными взносами с активами на сумму 9,3 триллиона долларов США.

В руководстве подчеркивается, что участники и активы подвержены риску внутренних и внешних угроз кибербезопасности, и что фидуциары ERISA обязаны принимать соответствующие меры для минимизации этих рисков.

Руководство состоит из трех частей:

(i) Советы по найму поставщика услуг,

(ii) передовой опыт программы кибербезопасности и

(iii) Советы по онлайн-безопасности.

Хотя это руководство предназначено, чтобы помочь спонсорам, фидуциарам и участникам защитить свои пенсионные пособия и личную информацию, следует также отметить упоминание фидуциарных обязанностей. Мы рекомендуем доверенным лицам ERISA ознакомиться с этим руководством, поскольку несоблюдение этих рекомендуемых практик или, по крайней мере, внедрение сопоставимых процедур не будет выглядеть хорошо в случае нарушения и требований участников или других сторон о слабых процедурах безопасности.

Кроме того, мы проверяем соглашения с поставщиками услуг, и часто поставщики услуг полностью отказываются от ответственности за нарушения кибербезопасности в первоначальных проектах этих соглашений. Если вы не просматривали контракты с вашим поставщиком услуг по кибербезопасности, это руководство будет хорошим поводом для этого. Руководство предназначено для работы с другими руководствами EBSA по электронным записям и раскрытию информации». ***(John Ludlum. In the Darkness at the Edge of Town…Cybersecurity Guidance for Plan Participants, Record-Keepers, and Plan Sponsors From The EBSA // Holland & Hart LLP (https://www.employeebenefitslawblog.com/in-the-darkness-at-the-edge-of-towncybersecurity-guidance-for-plan-participants-record-keepers-and-plan-sponsors-from-the-ebsa/#page=1). 15.04.2021).***

***

«Юта недавно внесла поправки в свой закон об уведомлении о нарушениях, чтобы обеспечить определенную защиту компаниям, которые страдают от утечки данных. Теперь это второй штат после Огайо, который включает такие положения. В частности, организации, которые создают и в разумных пределах соблюдают письменную программу кибербезопасности, могут иметь положительную защиту от судебного разбирательства, возникшего в результате утечки данных. Для применения безопасной гавани письменная программа кибербезопасности должна:

разрабатываться для защиты от безопасности, конфиденциальности и целостности личной информации, а также от ожидаемых угроз и опасностей;

разумно соответствовать признанной структуре кибербезопасности, такой как NIST 800-171 или 800-53, ISO 27000, PCI DSS, и федеральным законам, таким как HIPAA и GLBA (среди прочих); а также

соответствовать «масштабу и размаху» компании, информации, которую она собирает, видам деятельности, которыми она занимается, а также имеющимся ресурсам и инструментам.

Даже если существует письменная программа кибербезопасности, есть определенные исключения. Например, если организация получила фактическое уведомление об угрозе безопасности личной информации. Или, если он не предпринял действий в разумные сроки, предпринять известные меры по исправлению положения для защиты личной информации». ***(Julia Kadish, Liisa Thomas. Utah Creates Data Breach Safe Harbor // Sheppard Mullin (https://www.eyeonprivacy.com/2021/04/utah-safe-harbor/#page=1). 12.04.2021).***

***

«В начале марта Департамент финансовых услуг штата Нью-Йорк («DFS») подписал приказ о согласии, требующий, чтобы компания по жилищной ипотеке выплатила 1,5 миллиона долларов за несоблюдение Положения о кибербезопасности, часть 500 раздела 23 Кодекса штата Нью-Йорк. Крутой финансовый штраф в приказе о согласии является суровым напоминанием компаниям, подпадающим под действие Части 500, о том, что они должны уделять первоочередное внимание соблюдению.

В феврале 2017 года в Нью-Йорке был принят закон, обязывающий финансовые компании внедрять и сообщать подробную структуру, направленную на защиту конфиденциальности данных потребителей. Часть 500 Раздела 23 Кодекса штата Нью-Йорк применяется к любой организации, деятельность которой регулируется DFS. Это регулирование в значительной степени влияет на финансовую, банковскую и страховую отрасли США. Субъекты, нарушающие этот закон, могут понести штраф в размере до 250 000 долларов США за каждый день нарушения или одного процента от общих банковских активов.

Компании, подпадающие под действие Части 500, ожидают результатов по этому вопросу, потому что это вопрос первого впечатления. 3 марта 2021 года DFS достигла своего первого полного урегулирования в соответствии с Частью 500, касающейся жилищных ипотечных услуг. DFS и Служба жилищного ипотечного кредитования согласились разрешить этот вопрос без дальнейших разбирательств. В результате жилищная ипотека должна уплатить гражданский денежный штраф в размере 1,5 миллиона долларов в течение десяти дней с момента исполнения приказа о согласии. Принимая это решение, DFS оценила степень, в которой жилищная ипотека сотрудничала с DFS в своем расследовании, финансовые ресурсы и добросовестность проведения расследования, серьезность нарушения и общественные интересы. Установив этот серьезный финансовый штраф, DFS послала очень четкий сигнал другим компаниям, подпадающим под действие Части 500: соблюдайте, подчиняться и подчиняться. Кроме того, DFS ввела ряд корректирующих мер в отношении жилищной ипотеки, направленных на предотвращение будущих инцидентов путем обеспечения безопасности своих систем кибербезопасности и данных клиентов. Эти меры включают план реагирования на инциденты кибербезопасности, оценку рисков кибербезопасности в течение 90 дней с момента заказа, а также программы обучения и мониторинга в течение 90 дней с момента заказа». ***(Alan Friel, Ann J. LaFrance, Katie Sharpless. DFS Enters Into $1.5 Million Consent Order With Residential Mortgage Company In Wake of Data Breach // Squire Patton Boggs (https://www.securityprivacybytes.com/2021/04/dfs-enters-into-1-5-million-consent-order-with-residential-mortgage-company-in-wake-of-widespread-data-breach/). 13.04.2021).***

***

«4 марта 2021 года Счетная палата правительства США («GAO») опубликовала отчет под названием «Кибербезопасность систем вооружения: руководство поможет программам Министерства обороны США лучше сообщать о требованиях подрядчикам» («Отчет»). 1 Отчет следует за предыдущим отчетом за 2018 год («Отчет за 2018 год»), в котором было обнаружено, что Министерство обороны («DoD») только недавно начало уделять приоритетное внимание кибербезопасности систем вооружений и что в процессе приобретения DoD изо всех сил пытались предоставить оружие, которое было бы устойчивым к киберпространству. 2 В последнем отчете GAO были рассмотрены шаги, предпринятые Министерством обороны для улучшения кибербезопасности систем оружия, и обнаружено, что, несмотря на некоторый прогресс, некоторые

программы изо всех сил пытались включить требования кибербезопасности в контракты.В Отчете рекомендуется, чтобы армия, флот и корпус морской пехоты, в частности, предоставили рекомендации о том, как их основные программы оборонных закупок должны включать в контракты индивидуальные требования кибербезопасности.

Отчет является одним из нескольких недавних событий в растущем внимании правительства США к соблюдению требований кибербезопасности и стандартам в государственных контрактах. Подрядчики и субподрядчики, поддерживающие программы систем вооружений, должны быть готовы к тому, что более подробные требования к кибербезопасности будут включены в существующие контракты и заявки на заключение будущих контрактов.

Выводы и рекомендации отчета

После отчета за 2018 год Министерство обороны добилось больших успехов в улучшении кибербезопасности своих систем вооружения.Во-первых, Министерство обороны получило более широкий доступ к кибернетической экспертизе, сосредоточив внимание на найме и удержании квалифицированного персонала в рамках своих кадровых ресурсов.Во-вторых, Министерство обороны расширило использование кибер-оценок, проводя тестирование кибербезопасности на протяжении всего процесса приобретения.В-третьих, DoD более точно адаптировал свои меры безопасности к аналогичным типам систем, включив структуру управления рисками («RMF»), шестиэтапный процесс для управления и снижения рисков кибербезопасности для систем DoD.Наконец, Министерство обороны выпустило подробную политику или руководство по внедрению RMF.

Несмотря на этот прогресс, в отчете было обнаружено, что Министерство обороны все еще изо всех сил пытается включить требования кибербезопасности в свои процессы и контракты на приобретение систем оружия.В соответствующей части политики и руководства армии, флота и морской пехоты обсуждают необходимость требований к кибербезопасности, но не включают подробное руководство относительно того, как контракты на системы вооружения должны включать эти требования и более широкие цели кибербезопасности.

GAO обнаружило, что многие из проверенных им контрактов не содержали требований к кибербезопасности, в то время как другие, которые действительно содержали требования к кибербезопасности, четко не определяли, как выполнять эти требования.Например, некоторые контракты включали в себя общие формулировки, требующие от подрядчиков «киберустойчивости» или «соблюдения RMF» без каких-либо дополнительных подробностей о том, как подрядчик должен достичь такого стандарта или чего правительство хочет от киберсистемы.Кроме того, контракты на другие системы оружия не определяли требований кибербезопасности в объективных терминах, а также не содержали проверенных контрактов количественных и объективных критериев того, как правительство могло бы проверить и гарантировать, что подрядчик выполняет контрактные требования кибербезопасности.

В отчете было обнаружено, что отсутствие четких и объективных спецификаций кибербезопасности в контрактах на системы оружия создает риск того, что после заключения контракта потребуется внести изменения, что

потребует согласования справедливых корректировок, что приведет к задержкам и увеличению затрат.Таким образом, отсутствие значимых требований кибербезопасности в процессе приобретения систем оружия означает, что системы вооружений Министерства обороны могут столкнуться с трудностями при своевременной доставке оружия, которое является кибер-устойчивым и способным выполнять задачи в случае кибератаки.

В отчете рекомендуется, чтобы армия, флот и корпус морской пехоты3установили твердые, четкие и практически выполнимые кибер-требования на раннем этапе процесса приобретения, и чтобы эти службы использовали ходатайства для сообщения требований кибербезопасности, которые подрядчики будут использовать для разработки и производства систем оружия.В свою очередь, эти требования кибербезопасности затем будут отображаться как системные требования к производительности и спецификации в заключенных контрактах. В отчете также рекомендовалось Министерству обороны разработать рабочий процесс для проверки соблюдения подрядчиками этих договорных требований к кибербезопасности.

Что это означает для подрядчиков

Подрядчики, работающие над системами вооружения Министерства обороны, должны быть готовы к изменениям в процессе приобретения систем вооружений в будущем.Министерство обороны согласилось с рекомендациями GAO и согласилось с тем, что следует разработать руководство по программам приобретения, чтобы включить в контракты индивидуальные требования к кибербезопасности систем оружия, критерии приемки и процессы проверки.Эти требования к кибербезопасности могут появляться во всех аспектах цепочки поставок систем вооружения Министерства обороны США, а это означает, что любой подрядчик, субподрядчик или поставщик, занятый в работе по поддержке систем вооружения Министерства обороны, может увидеть в своих контрактах новые или более подробные требования к кибербезопасности.

Такие требования добавят к и без того сложной и развивающейся структуре кибербезопасности, по которой подрядчики должны ориентироваться, включая следующие недавние изменения в стандартах кибербезопасности:

Сертификация модели зрелости кибербезопасности и методология оценки NIST SP 800-171 DoD.В прошлом году DoD издало временное правило, чтобы дополнить свою программу сертификации модели зрелости кибербезопасности (CMMC) методологией оценки DoD.Временное правило внесло поправки в Дополнение к Положению об оборонных федеральных закупках («DFARS»), чтобы обеспечить двухэтапный процесс проверки подрядчиков, требуя, чтобы подрядчики были сертифицированы с помощью методологии оценки NIST SP 800-171 Министерства обороны США перед тем, как пройти через полную структуру CMMC.4Мы ранее обсуждали это развитие более подробноздесь.

НИСТ СП 800-53. Национальный институт науки и технологий («NIST») недавно выпустил существенно переработанную версию своего стандарта кибербезопасности, NIST SP 800-53, «Контроль безопасности и конфиденциальности для информационных систем и организаций».5Хотя NIST SP 800-53 применяется к правительственным системам и организациям США (NIST SP

800-171 устанавливает производный набор стандартов кибербезопасности для подрядчиков), правительство сделало соответствие стандартам NIST SP 800-53 применимым ко многим подрядчикам посредством договорных требований., а изменения к SP 800-53, вероятно, будут отражены в будущих версиях SP 800-171 и модели CMMC.

V&E внимательно следит за ожиданиями подрядчиков, связанными с кибербезопасностью, и готова ответить на любые ваши вопросы по этим и другим событиям в этой области». ***(Dan Graham, Devika Kornbacher, John Satira, Funmi Anifowoshe-Manning. GAO Urges Changes as Weapon Systems Cybersecurity Continues to Lag // Vinson & Elkins LLP (https://www.velaw.com/insights/gao-urges-changes-as-weapon-systems-cybersecurity-continues-to-lag/). 08.04.2021).***

***

«Сенаторы Гэри Петерс (Мичиган), Джон Хувен (Северная Дакота) и Джеки Розен (штат Невада) недавно вновь представили Закон о федеральной программе ротации кибербезопасности, который направлен на развитие и удержание высококвалифицированных федеральных кадровых специалистов в области кибербезопасности.

Сенаторы утверждают, что агентства федерального правительства сталкиваются с растущими киберугрозами, пытаясь нанять и удержать квалифицированных сотрудников по кибербезопасности.

«Недавние нарушения нашей федеральной киберинфраструктуры, которые поставили под угрозу национальную безопасность, показывают, что нашему правительству нужны интегрированные федеральные кибернетические кадры, обладающие знаниями и навыками для противодействия все более изощренным угрозам». Об этом заявил Петерс, председатель Комитета внутренней безопасности и по делам правительства. «Я горжусь тем, что вновь представил этот здравый закон, который укрепит штат сотрудников федерального правительства по кибербезопасности, предоставив кибер-сотрудникам уникальные возможности профессионального развития, пока они продолжают служить нашей стране».

Законопроект предусматривает создание программы ротации гражданского персонала для специалистов по кибербезопасности в федеральных агентствах, позволяющей сотрудникам работать в нескольких государственных учреждениях, приобретать опыт, выходящий за рамки основного назначения, и расширять свои профессиональные сети.

«Наш двухпартийный законопроект поможет федеральному правительству обучать и удерживать профессионалов в области кибербезопасности для удовлетворения растущего спроса», - сказал Хувен. «Разрабатывая программу ротации кибер кадровых ресурсов, этот закон позволит федеральным служащим работать в различных государственных учреждениях и расширять свои навыки. Все дело в том, чтобы у федерального правительства были профессионалы, необходимые для решения проблем кибербезопасности нашей страны».

Законодатели отметили, что законопроект также будет привлекать и удерживать экспертов по кибербезопасности, предлагая гражданским служащим возможности для карьерного роста, расширения профессионального опыта и

развития сетей сотрудничества, получая опыт и внося свой вклад в кибер-миссию за пределами местных агентств». ***(Douglas Clark. Measure bolsters federal cybersecurity workforce // Homeland Preparedness News (https://homelandprepnews.com/stories/67069-measure-bolsters-federal-cybersecurity-workforce/). 16.04.2021).***

***

«Законодатели Флориды близки к принятию закона, который пересмотрит систему управления кибербезопасностью штата в то время, когда он имеет дело с последствиями инцидентов, таких как взлом местного водоочистного сооружения и потенциально дорогостоящая атака с помощью программ-вымогателей на один из крупнейших школьных округов.

Законопроект HB1297 добавит дополнительные обязанности по обеспечению кибербезопасности Флоридской цифровой службе, агентству, которое было создано в прошлом году, когда в штате проводился один из частых капитальных ремонтов ИТ. Среди новых обязанностей молодого агентства будет разработка ежегодных тренингов по кибербезопасности для государственных служащих, создание Консультативного совета по кибербезопасности в составе 19 членов и разработка плана для штата, который будет обновляться ежегодно. Законопроект основан на отчете, опубликованном в январе целевой группой из 15 человек, в которую входили лейтенант Жаннетт Нуньес, главный информационный директор штата Джеймс Грант и представители правоохранительных органов, а также представители университетов и корпораций Флориды, таких как Walt Disney World.

В новый совет войдут многие из тех же членов, что и рабочая группа, а также главный сотрудник по информационной безопасности штата - должность, которая была вакантной с декабря прошлого года, когда ее бывший руководитель Томас Вон покинул правительство штата, чтобы стать директором по информационной безопасности столицы. город Таллахасси. В него также войдут три представителя критически важных объектов инфраструктуры, по крайней мере, один из которых должен быть из водоочистных сооружений. Власти штата и федеральные власти все еще расследуют февральский инцидент, в ходе которого хакер якобы попытался поднять уровень гидроксида натрия до опасного уровня на заводе в городе Олдсмар.

Между тем, государственные школы округа Бровард, шестой по величине округ страны K-12, в начале этого месяца подверглись атаке с использованием программ-вымогателей, потребовавшей 40 миллионов долларов, что является рекордной суммой. (В округе заявили, что не будут платить, хотя на короткое время пытались договориться с атакующей его бандой.)

HB1297 уже был единогласно одобрен несколькими комитетами Палаты представителей Флориды, и соответствующий закон проходит через Сенат штата. Законопроект также движется по мере того, как законодатели рассматривают план расходов на 2022 финансовый год, который включает увеличение финансирования кибербезопасности на 31,6 миллиона долларов, которое поддержит рекомендации в январском отчете целевой группы, включая дополнительные инструменты обнаружения конечных точек и оценки угроз, усиление защиты промышленных

предприятий. системы управления, например, на водных установках, обновление правительственных веб-сайтов до доменов.gov и 15 новых позиций во Флоридской цифровой службе.

Однако увеличение расходов штата на кибербезопасность входит в список программ, которые будут финансироваться только в том случае, если Флорида получит достаточную помощь от пандемии, согласно законопроекту об ассигнованиях». ***(Benjamin Freed. Florida lawmakers consider cybersecurity overhaul // StateScoop (https://statescoop.com/florida-lawmakers-consider-cybersecurity-overhaul/). 12.04.2021).***

***

«Представители Национального нефтяного совета (National Petroleum Council, NPC) опубликовали отчет Dynamic Delivery: America's evolving oil and natural gas transportation infrastructure («Динамические поставки: развивающаяся инфраструктура транспортировки нефти и природного газа в Америке»), призванный помочь компаниям и организациям в нефтегазовой промышленности лучше реагировать на кибератаки.

Старший вице-президент по технологиям, процессам и управлению рисками компании Plains All American Pipeline Эл Линдсет (Al Lindseth) пояснил, потенциальная кибератака на OT-сети (Operational Technology) может привести к огромным экономическим последствиям для компаний, включая последствия для окружающей среды, а также здоровья и безопасности людей.

Один из ключевых выводов отчета касается важности сотрудничества отраслевых компаний и государственных учреждений с целью снижения киберрисков. Так называемый подход SMART призывает к обмену информацией как в сфере IT, так и в сфере OT. Подход SMART относится информации, которая является «конкретной, измеримой, действенной, актуальной и своевременной».

«Мы можем развивать доверие в отношениях, и мы можем больше делиться информацией с другими. Особенно важно иметь возможность делиться друг с другом не только обычными, простым данными, но и более конфиденциальной и конкретной информацией, которая может служить на благо всего и повышать безопасность всей отрасли», — отметила исполнительный директор Центра обмена и анализа информации о нефти и природном газе (ONG-ISAC) Анжела Хаун (Angela Haun)». ***(Национальный нефтяной совет США опубликовал отчет о рисках кибербезопасности в нефтегазовой отрасли // SecurityLab.ru (https://www.securitylab.ru/news/518965.php). 15.04.2021).***

***

«Университет Арканзаса в Литл-Роке проведет престижный общенациональный летний лагерь для учащихся младших и старших классов, желающих получить новейшие навыки в востребованной области кибербезопасности. Лагерь предлагается студентам бесплатно…

Программа спонсируется грантом в размере 100 000 долларов США от Агентства национальной безопасности и предоставляет одни из лучших учебных курсов по кибербезопасности для учащихся средних школ от ведущих

преподавателей по всей стране. У студентов будет возможность поработать с практическими кибератаками и защитными тренировками на Cyber Arena и услышать мнение всемирно известных экспертов в области кибербезопасности. Студенты могут присутствовать на программе виртуально или лично на Cyber Arena в колледже науки, технологий, инженерии и математики Donaghey.

«Студенты научатся думать как хакеры и останавливать киберпреступников на своем пути», - сказала Сандра Лейтерман, управляющий директор UA Little Rock Cyber Arena. «Каждый день будет выступать всемирно известный эксперт по кибербезопасности и лучшие практические занятия по кибербезопасности в регионе».

Этот двухнедельный лагерь посвящен концепциям кибербезопасности GenCyber. Участники услышат от отраслевых экспертов о возможностях карьерного роста и узнают о кибербезопасности с помощью современных практических занятий, которые позволят студентам испытать кибератаки как со стороны жертвы, так и со стороны противника». ***(Angelita Faller. UA LITTLE ROCK TO HOST FIRST EVER NSA GENCYBER CYBERSECURITY CAMP IN ARKANSAS // UA Little Rock (https://ualr.edu/news/2021/04/27/nsa-gencyber-cybersecurity-camp/). 27.04.2021).***

***

«После обращения президента Байдена к Конгрессу вчера вечером, в котором он дважды упомянул кибербезопасность в качестве приоритета, сегодня циркулируют новости о том, что исполнительный указ о кибербезопасности неизбежен. Эта новость является долгожданным и давно назревшим шагом на пути к стандартизации и структурированию кибербезопасности.

Энн Нойбергер, заместитель советника по национальной безопасности по кибербезопасности и новейшим технологиям, говорит, что порядок будет похож на Национальный совет по безопасности на транспорте (NTSB) для кибербезопасности.

Что мы можем узнать о том, как заблаговременно предупреждать о таких инцидентах она недавно сказала репортерам. Она также отмечает, что это распоряжение станет отправной точкой, которая в конечном итоге должна проникнуть и на потребительский рынок. «Если мы начнем стимулировать безопасность, тогда компании [и] рынок будут уделять ей приоритетное внимание, потому что больше людей будут покупать продукт», она сказала.

С моей точки зрения, я рад, что эта тема наконец- то замкнулась. В 2013 году Крис Висопал затронул именно эту тему в своем программном докладе на RVASec, где он обсудил «Будущее разделения правительства».

Фактически, Крис начал информировать федеральное правительство 23 года назад, когда он и несколько его коллег из хакерского аналитического центра L0pht свидетельствовали перед Конгрессом о попытках выявить риски и угрозы кибербезопасности. Восемь лет спустя я присоединился к Крису, когда он запустил Veracode, чтобы начать решать критическую проблему безопасности программного обеспечения Вместе мы сосредоточились на том, чтобы помочь разработчикам и

командам безопасности не только найти, но и исправить уязвимости в их программном обеспечении (разработанном собственными силами, с открытым исходным кодом или приобретенном сторонними организациями).

Буквально в прошлом месяце, в Международный женский день, я встретился с репортером The New York Times по кибербезопасности Николь Перлрот и членом правления OWASP Ванданой Верма, чтобы обсудить эту тему на подкасте конференции RSA разделяя это, недавнее исследование Veracode показало, что 66 процентов приложений не соответствуют стандартам OWASP Top 10, что означает, что они имеют серьезную уязвимость. Это подчеркивает, что предстоит проделать работу, и мы должнывстроить тестирование безопасности в жизненный цикл разработки программного обеспечения, чтобы, когда разработчики пишут код, они писали безопасно. В этом обсуждении Перлрот сказал: «Мы не можем пытаться исправить эти исправления после того, как уязвимый код уже попал в руки пользователей, но также и в критически важную инфраструктуру». Мы должны думать о безопасности. и дизайн безопасности с самого начала. Надо с самого начала привлекать инженеров по безопасности.

Чтобы сделать программное обеспечение более безопасным, необходимо интегрировать безопасность в жизненный цикл разработки программного обеспечения и обучить разработчиков. Нам не следует ожидать безопасного кода, если мы не установили ясность в отношении внешнего вида продукта, не снабдили разработчиков правильными инструкциями, необходимыми знаниями и необходимыми инструментами.

Указ был издан давно, и я надеюсь, что он устанавливает, какими должны быть правильные ожидания и подотчетность. Мы должны структурировать и стандартизировать кибербезопасность и безопасность программного обеспечения, и есть ряд отличных примеров того, как это было успешно сделано. Один из наших клиентов, поставщик образовательного программного обеспечения, присоединился к программе Veracode Verified, чтобы предоставить доказательства своих процессов безопасности и иметь право вести дела с системой государственных школ Нью-Йорка. Другими словами, покупатель возложил на разработчика программного обеспечения ответственность за демонстрацию безопасного процесса разработки программного обеспечения, и с помощью стороннего тестирования, например, с помощью программы Veracode Verified, они смогли это сделать.

Учитывая продолжающееся воздействие нарушений на федеральное правительство и компании, пришло время заняться этим вопросом целенаправленно и энергично. Мы должны установить общий стандарт кибербезопасности, который устраняет одну из основных первопричин нарушений уязвимости в программном обеспечении. Поскольку мы живем, работаем и играем в цифровом мире все больше и больше, это необходимо, наконец, сделать это». ***(Executive Order on Cybersecurity Is Imminent: It's Been a Long Time Coming // Security Boulevard (https://securityboulevard.com/2021/04/executive-order-on-cybersecurity-is-imminent-its-been-a-long-time-coming/). 29.04.2021).***

***

«Исследователи из восьми университетов Вирджинии скоро примут участие в финансируемых государством исследовательских проектах по кибербезопасности и автономных транспортных средствах на сумму 1 миллион долларов в рамках исследовательской инициативы в масштабе штата, сообщил в четверг Virginia Tech.

Все проекты предназначены для использования в различных аспектах работы специалистов по кибербезопасности, включая био-кибербезопасность - новую область, связанную с здравоохранением и данными о состоянии здоровья, - и кибербезопасность автономных транспортных средств, а также несколько проектов, посвященных развитию стартапов в области кибербезопасности и расширению стажировок в области информации. индустрия безопасности.

Участвующие университеты - Университет Джорджа Мейсона, Университет Лонгвуда, Университет Мэримаунт, Университет Олд-Доминион, Университет Рэдфорда, Университет Вирджинии, Технологический институт Вирджинии и Уильям и Мэри - заставят студентов работать над реальными проектами кибербезопасности, такими как создание Кибербезопасности. Мониторинг центра управления и контроля в порту Вирджинии и практическое обучение на испытательном стенде системы безопасности киберпитания Virginia Tech - еще один проект, запуск которого запланирован на этот год, который позволит студентам изучить способы защиты сетей 5G. Студенты William and Mary будут работать в паре с компаниями, работающими с данными, связанными с риском кибербезопасности.

Список проектов будет финансироваться через Commonwealth Cyber Initiative, организованную государством сеть исследователей из колледжей и университетов, которая базируется в кампусе Virginia Tech в Блэксбурге, штат Вирджиния. CCI был подписан законодательными органами штата в 2018 году с целью развития кадровых ресурсов и привлечения компаний, занимающихся кибербезопасностью. Штат одобрил финансирование сети в размере 17,5 млн долларов в апреле 2020 года на 2021 финансовый год». ***(Ryan Johnston. Eight Virginia universities announce cybersecurity workforce projects // EdScoop (https://edscoop.com/eight-virginia-universities-announce-cybersecurity-workforce-projects/). 29.04.2021).***

***

Країни ЄС та Великобританія

«Информационные технологии все чаще подвергаются потенциально злонамеренным намерениям различных групп и отдельных лиц. Следовательно, систематические и скоординированные усилия по повышению возможностей кибербезопасности являются ключом к безопасному цифровому обществу.

Система кибербезопасности Хорватии представляет собой сложную межотраслевую сеть институтов и нормативных актов, которая постоянно развивается, но соответствует требованиям, полученным в результате членства

страны в Европейском союзе и Организации Североатлантического договора (НАТО).

Это вторая статья из серии о регулировании кибербезопасности в Хорватии. (1)

Учреждения Закона об информационной безопасности

Первым правовым актом, регулирующим вопросы кибербезопасности в Хорватии, был Закон об информационной безопасности (Официальный вестник 79/2007), который был принят в 2007 году. Этот закон заложил основы кибербезопасности в общественной киберсфере и учредил три органа, которые играют ключевые роли в Хорватии. политика кибербезопасности:

Офис Совета национальной безопасности (ONSC);

Бюро безопасности информационных систем (ISSB); а также

Группа реагирования на компьютерные чрезвычайные ситуации (CERT).

ONSC

В соответствии с Законом об информационной безопасности ONSC стал органом национальной безопасности, отвечающим за координацию национальных измерений и стандартов ЕС и НАТО для защиты секретной и несекретной информации в государственном секторе. ONSC является основным органом хорватской системы безопасности и разведки. Он выполняет задачи Совета национальной безопасности и Совета по координации служб безопасности и разведки и информирует президента и премьер-министра о работе служб безопасности и разведки.

ISSB

Закон об информационной безопасности поручил ISSB координировать меры предотвращения и реагирования в отношении угроз безопасности информационных систем в государственном секторе. ISSB - это центральный государственный орган, отвечающий за техническую сторону информационной безопасности государственных органов. Это включает в себя управление:

стандарты информационной безопасности;

аккредитация безопасности; а также

зашифрованный материал, используемый во время обмена секретной информацией и аналогичных задач.

Директора ISSB назначаются правительством на основании предложений Совета по координации служб безопасности и разведки.

CERT

Закон об информационной безопасности учредил CERT как отдел в рамках Хорватской академической и исследовательской сети. CERT отвечает за предотвращение угроз безопасности и защиту всех общедоступных информационных систем в Хорватии. Его основная задача - обрабатывать инциденты компьютерной безопасности, в которых одна из сторон находится в Хорватии (то есть стороны, которые имеют домен.hr или находятся в диапазоне адресов хорватского интернет-протокола).

Дополнительные функции ONSC, ISSB и CERT

Закон о кибербезопасности операторов основных услуг и поставщиков цифровых услуг 2018 г. (Официальный вестник 64/2018), который был перенесен

из Директивы ЕС по сетевой и информационной безопасности (2016/1148 / EU), дал у трех органов дополнительные национальные функции. ONSC стал единым национальным контактным лицом, в то время как ISSB и CERT стали органами национальной группы реагирования на инциденты компьютерной безопасности с аналогичными задачами предотвращения и реагирования.

Институты Национальной стратегии кибербезопасности

Принятие в 2015 году Национальной стратегии кибербезопасности потребовало создания межведомственного органа для мониторинга ее реализации и установления связи между компетентными учреждениями в правительстве и государственном секторе. В 2016 году были созданы два межведомственных органа для управления реализацией целей и показателей Национальной стратегии кибербезопасности, а также для решения всех соответствующих национальных вопросов кибербезопасности:

Национальный совет по кибербезопасности; а также

Координационная группа по оперативной и технической кибербезопасности.

Национальный совет по кибербезопасности Национальный совет по кибербезопасности состоит из 16 представителей следующих государственных учреждений:

ОНБК;

Центральное государственное управление по развитию цифрового общества;

Агентство безопасности и разведки;

ISSB;

Оперативно-технический центр телекоммуникационного наблюдения;

Хорватская академическая и исследовательская сеть;

CERT;

Регулирующий орган Хорватии для сетевой индустрии;

Хорватский национальный банк; а также

Хорватское агентство по защите личных данных.

Представитель ONSC выступает в качестве президента. Национальный совет по кибербезопасности подотчетен правительству и отвечает за реализацию трех мер по управлению кибер-кризисами.

Координационная группа по оперативной и технической кибербезопасности Группа по координации оперативной и технической кибербезопасности поддерживает деятельность Национального совета по кибербезопасности посредством:

мониторинг национального киберпространства для обнаружения угроз, которые могут привести к кибер-кризису;

отчетность о состоянии мер кибербезопасности;

предложение планов действий на случай кибер-кризисов; а также

выполнение других задач в соответствии с установленными программами.

Координационная группа по оперативной и технической кибербезопасности состоит из восьми членов, некоторые из которых являются представителями организаций, которые также представлены в Национальном совете по кибербезопасности. Представитель Министерства внутренних дел действует как координатор. Координационная группа по оперативной и технической

кибербезопасности подотчетна Национальному совету по кибербезопасности и участвует в реализации мер, за которые совет несет ответственность». ***(Ivana Manovelo. Cybersecurity: overview of relevant institutions // Law Business Research (https://www.internationallawoffice.com/Newsletters/Tech-Data-Telecoms-Media/Croatia/Maei-Partners/Cybersecurity-overview-of-relevant-institutions). 02.04.2021).***

***

«Правительство Великобритании опубликовало свой ответ на призыв высказать мнения о предлагаемом законодательстве о кибербезопасности подключенных потребителей продуктов 21 апреля 2021 года, подтвердив планы по принятию новых законов, устанавливающих обязательные требования кибербезопасности для продуктов, продаваемых «по всей Великобритании».

Согласно предложенным новым правилам, определенные подключенные потребительские устройства, продаваемые в Великобритании, должны будут соответствовать следующим трем требованиям, устанавливающим «минимальный базовый уровень кибербезопасности»:

Пароли должны быть уникальными, и их нельзя сбрасывать до универсальных заводских настроек.

Производители должны предоставить общедоступную точку контакта, чтобы любой мог сообщить об уязвимости.

Клиенты должны быть проинформированы в торговой точке о том, как долго устройство будет получать обновления программного обеспечения безопасности.

В ответе отмечается, что эти требования были взяты из трех основных руководящих принципов Кодекса практики безопасности потребительского Интернета вещей и положений Европейского стандарта ETSI (EN) 303 645 и согласуются с ними.

Предлагаемые новые правила будут применяться к широкому спектру подключенных потребительских товаров, включая интеллектуальные колонки, интеллектуальные телевизоры, подключенные дверные звонки, смартфоны, подключенные игрушки и подключенные носимые фитнес-трекеры (среди многих других).

Однако, согласно последним предложениям, некоторые устройства теперь будут изначально освобождены от уплаты, включая настольные компьютеры, ноутбуки и планшеты без сотовой связи, которые правительство сочло «неуместным включать в ожидании дальнейшего расследования». В исходных предложениях, опубликованных для июльского конкурса 2020 г. Однако в ответе отмечается, что после отзывов, полученных от заинтересованных сторон, правительство признает «уникальные проблемы, с которыми производители этих продуктов столкнутся при соблюдении нашего законодательства, и проведет дальнейшую работу по взаимодействию и анализу, прежде чем предпринимать какие-либо действия по добавлению этих устройств в список. объем регулирования в будущем».

Правительство также отметило, что предлагаемый закон позволит ввести дополнительные требования безопасности в будущем, которые могут включать аутентификацию пользователей, отчеты об уязвимостях, обновления программного обеспечения и принципы проектирования безопасности для программного и аппаратного обеспечения (среди других примеров, приведенных в ответе).

Предложения, опубликованные для запроса доказательств, проведенного в прошлом году, предвещали очень короткие переходные периоды после принятия закона (9 месяцев для первого требования, 3 месяца для второго, 6 месяцев для третьего). В ответе на запрос мнений отмечается, что «после королевского согласия правительство предоставит соответствующим экономическим субъектам соответствующий льготный период для корректировки своей деловой практики до того, как предполагаемый закон полностью вступит в силу».

Что касается того, что будет дальше, правительство Великобритании в настоящее время разрабатывает законопроект, который будет внесен в парламент, «когда парламентское время позволит».

Учитывая первоначально предложенные короткие переходные периоды, производители, импортеры и дистрибьюторы рассматриваемых устройств должны внимательно следить за этим развитием по мере его продвижения.

Европейская комиссия также работает над рядом инициатив по кибербезопасности подключенных потребительских устройств, включая делегированный закон в соответствии с Директивой о радиооборудовании 2014/53 / EU (проект, который, как ожидается, будет опубликован в ближайшее время), потенциальную схему сертификации для IoT. устройства в соответствии с Законом ЕС о кибербезопасности (Регламент (ЕС) 2019/881) и новым горизонтальным законодательным актом (отмеченным как более долгосрочная мера)…» ***(UK government confirms plans to bring in mandatory cyber security requirements for connected consumer products // Productwise (https://products.cooley.com/2021/04/26/uk-government-confirms-plans-to-bring-in-mandatory-cyber-security-requirements-for-connected-consumer-products/#page=1). 26.04.2021).***

***

«Устойчивость, технологический суверенитет и лидерство важны для ЕС, и поэтому они рассматриваются в Стратегии кибербезопасности ЕС. Стремясь поддержать эту стратегию кибербезопасности, ENISA выпускает отчет, предназначенный для изучения цифровой стратегической автономии в ЕС, и предлагает направления будущих исследований.

Что такое цифровая стратегическая автономия?

Цифровую стратегическую автономию можно определить как способность Европы предоставлять продукты и услуги, предназначенные для удовлетворения конкретных потребностей и ценностей ЕС, избегая при этом влияния внешнего мира.

В цифровом мире такие потребности могут включать оборудование, программное обеспечение или алгоритмы, производимые как продукты и / или услуги, которые должны соответствовать ценностям ЕС и, таким образом,

сохранять справедливую цифровую экосистему при соблюдении конфиденциальности и цифровых прав.

Чтобы обеспечить соответствие источников таких продуктов и / или услуг потребностям и ценностям ЕС, у ЕС есть возможность самостоятельно производить их автономно или в случае, когда продукты и услуги приобретаются из третьих стран, сертифицировать их и подтверждать. их соответствие.

Однако в тех случаях, когда существует высокая зависимость от источников, ЕС по-прежнему должен иметь возможность управлять своей цифровой инфраструктурой, не оказывая при этом никакого возможного пагубного влияния. Следовательно, Европе необходимо сохранять способность самостоятельно производить свои критически важные продукты и услуги.

Короче говоря, цифровая стратегическая автономия означает способность ЕС оставаться автономным в определенных сферах общества, где используются цифровые технологии.

Почему такой ход?

Новые вызовы, вызванные цифровизацией его среды, вызывают вопросы о его способности сохранять право собственности и контроль над своими персональными данными, своими технологическими активами и своей политической позицией. Таковы основные аспекты, которые следует учитывать в рамках идеи цифровой стратегической автономии.

Кроме того, пандемия COVID-19 подчеркнула важность кибербезопасности и необходимость для ЕС продолжать инвестировать в исследования и разработки в цифровом секторе. В этом контексте в отчете устанавливаются и приоритизируются ключевые направления исследований и инноваций в области кибербезопасности.

Ключевые направления исследований: какие они?

В отчете определены следующие семь ключевых областей исследования:

Безопасность данных

Надежные программные платформы

Управление киберугрозами и реагирование

Надежные аппаратные платформы

Криптография

Ориентированные на пользователя методы и инструменты безопасности

Безопасность цифровой связи». ***(Research directions in cybersecurity to support a digital strategic autonomy // Help Net Security (https://www.helpnetsecurity.com/2021/04/27/digital-strategic-autonomy/). 27.04.2021).***

***

«Запланированное приобретение транснациональной компании ускорит ее рост во Франции и укрепит ее возможности в области кибербезопасности по всей Европе.

Консалтинговый гигант Accenture объявила о планах приобрести компанию Openminded, занимающуюся кибербезопасностью, за неизвестную сумму.

После завершения сделки около 100 высококвалифицированных профессионалов в области кибербезопасности войдут в штат Accenture Security, насчитывающий почти 7000 специалистов по всему миру.

Компания Openminded, основанная во Франции, была основана в 2008 году и помогает клиентам прогнозировать и снижать риски кибербезопасности, обнаруживать кибератаки и реагировать на них, а также применять передовые методы обеспечения соответствия нормативным требованиям.

Эта покупка позволит Accenture ускорить рост во Франции, а также расширить возможности кибербезопасности по всей Европе.

Глобальный руководитель Accenture Security Келли Бисселл заявила, что с каждым днем кибератаки становятся все более сложными, и компании должны полностью внедрить кибербезопасность на всех уровнях своего бизнеса.

«Приобретение Openminded подтверждает нашу приверженность использованию технологий и человеческой изобретательности, чтобы помочь клиентам быть уверенными и защищенными перед лицом постоянных изменений», - сказал он.

«Мы с нетерпением ждем возможности приветствовать команду Openminded в Accenture и помочь клиентам более эффективно защищаться от киберугроз во всей экосистеме - сейчас и в будущем».

Оливье Жирар, руководитель подразделения Accenture France и Benelux, добавил, что план по приобретению Openminded согласуется с «глобальной стратегией компании по предоставлению дифференцированных надежных услуг» клиентам на их местных рынках.

Основатель и генеральный директор Openminded Эрве Руссо сказал, что объединение усилий с Accenture - прекрасная возможность для его компании. «Альянс наших талантов и возможностей идеально использует наш опыт и позволит нам работать в глобальном масштабе. Сегодня борьба с кибератаками требует внедрения самых передовых технологий, а также человеческих ресурсов, чтобы сделать их эффективными», - сказал он.

Приобретение подлежит обычным условиям закрытия.

Accenture стала крупным поставщиком услуг в области кибербезопасности после приобретения подразделения Symantec по предоставлению услуг в области кибербезопасности в начале 2020 года. Компания продолжила расширяться в этой области за счет приобретений, включая приобретение бразильской компании Real Protect в области информационной безопасности в начале этого года.

К другим компаниям, которые Accenture добавила в свой портфель в 2021 году, относятся Cirrus со штаб-квартирой в Великобритании и компания облачной аналитики Core Complete, а также немецкая Fable + и калифорнийская Imaginea». ***(Jenny Darmody. Accenture to acquire French cybersecurity company Openminded // SILICONREPUBLIC (https://www.siliconrepublic.com/enterprise/accenture-openminded-france-cybersecurity). 30.04.2021).***

***

«Финансовые регуляторы продолжали наращивать свои усилия по разработке и защите финансовых данных. Народный банк Китая выпустил новые стандарты по расширению возможностей финансовых учреждений по обработке данных. Кроме того, несколько банков были наказаны за нарушение правил защиты данных в отношении обработки личной информации.

МІІТ по-прежнему уделяет особое внимание защите данных в мобильных приложениях. Помимо разработки специального постановления о защите данных для мобильных приложений, МИИТ и его местные отделения проводят непрерывные кампании по борьбе с нарушениями конфиденциальности данных операторами мобильных приложений.

Нормативные разработки

1. Опубликованы новые руководящие принципы по наращиванию потенциала данных в финансовой отрасли

9 февраля Народный банк Китая (НБК) опубликовал Руководство по наращиванию потенциала данных в финансовой отрасли. Руководящие принципы определяют разделение стратегии данных, управления данными, архитектуры данных, спецификации данных, защиты данных, качества данных, приложений данных и возможностей управления жизненным циклом данных. Руководящие принципы призваны предоставить финансовым учреждениям основу для работы с данными, направить финансовые учреждения по укреплению стратегического планирования данных, сосредоточить внимание на управлении данными и усилить защиту данных.

2. Общие требования к безопасности критически важного кибероборудования.

20 февраля Государственная администрация по регулированию рынка и Управление по стандартизации утвердили семь обязательных национальных стандартов (включая обязательный национальный стандарт телекоммуникаций) и внесли одну поправку в Общие требования к безопасности критически важного кибероборудования, которые вступят в силу 1 августа. 2021. Эти требования (включая требования к функциям безопасности и защите) служат важными стандартами для реализации Закона о кибербезопасности, касающегося требований безопасности критически важного кибероборудования. Требования к функциям безопасности состоят из 10 частей, в которых основное внимание уделяется обеспечению и совершенствованию технологии безопасности. возможности устройств. К ним относятся безопасность идентификации устройства, восстановление резервных копий и обнаружение неисправностей, предотвращение уязвимостей и вредоносных программ, безопасность запуска и обновления предустановленного программного обеспечения, идентификация и аутентификация пользователей, безопасность контроля доступа, безопасность аудита журналов, безопасность связи, безопасность данных и требования к паролям. Отдельно требования к защите сосредоточены на стандартизации возможностей

безопасности поставщиков критически важного киберборудования на протяжении всего жизненного цикла оборудования.

3. Пять проектов стандартов по национальной технологии информационной безопасности выпущены для общественного обсуждения.

3 февраля Секретариат Национального технического комитета по стандартизации информационной безопасности (NISSTC) выпустил два проекта стандартов на службу инстансных сообщений и экспресс-логистику для общественного обсуждения. Кроме того, 24 февраля NISSTC опубликовал для общественного обсуждения три проекта стандартов в отношении сервисов онлайн-покупок, сервисов интернет-платежей и онлайн-аудио- и видеосервисов. Эта серия стандартов устанавливает требования к типу, области применения, методам, условиям и защите данных при сборе, хранении, использовании, передаче и удалении. Они также предоставляют примеры классификации данных и руководство для операторов по регулированию деятельности с данными, а также для надзорных органов и сторонних оценочных агентств для осуществления надзора, управления и оценки.

4. Новые правила управления приложениями для усиления защиты личной информации будут опубликованы.

7 февраля Министерство индустрии и информационных технологий (МИИТ) объявила, что разрабатывает временные положения о защите личной информации приложений. Положения будут определять основные принципы информированного согласия и минимально необходимой защиты личной информации. Принцип информированного согласия требует, чтобы для деятельности по обработке личной информации, связанной с приложением, субъекты (т.е. Субъект, обрабатывающий данные) должны информировать пользователей о правилах обработки личной информации в ясной и понятной форме, а пользователь должен добровольно ясно их согласие. Минимально необходимый принцип требует, чтобы во время обработки личной информации было четкое и разумное согласие, и оно не должно выходить за рамки согласия пользователей или не иметь отношения к сценариям обслуживания.

Развитие правоприменения

1. Выпущена вторая группа приложений 2021 года, признанных нарушающими права пользователей, всего 11-я группа.

5 февраля МИИТ опубликовал уведомление о приложениях, которые нарушают права пользователей, злоупотребляя микрофонами, адресными книгами и фотоальбомами. Он отметил, что 26 приложений не приняли необходимых мер по исправлению положения, причем крайний срок для этого - 10 февраля. Если исправление не будет произведено в срок, МИИТ организует и проведет соответствующие работы по утилизации в соответствии с законами и постановлениями. Проблемы с приложениями были связаны с нарушениями личной информации мобильного телефона, частыми и чрезмерными запросами разрешений, обязывающими пользователей использовать функцию целевых push-уведомлений, и неадекватным указанием пользователям информации о приложении на платформе распространения приложений.

2. Из магазина приложений было удалено 37 приложений с нарушением прав пользователей.

3 февраля MIIT объявила, что удалила из магазина приложений 37 приложений, нарушающих права пользователей, и не приняла необходимых мер по исправлению ситуации. Удаленные приложения собирают личную информацию сверх необходимого объема и были вовлечены в другие проблемы, нарушающие права пользователей. Напомним, что в течение двух лет подряд MIIT проводил специальные меры по исправлению ситуации в отношении приложений, которые незаконно обрабатывали личную информацию пользователей. Кроме того, MIIT также объявил, что усилит усилия по исправлению ошибок, способствуя разработке соответствующих стандартов и активно применяя новые технологии, такие как искусственный интеллект и большие данные, для содействия созданию национальной платформы тестирования технологий приложений.

3. Администрация связи провинции Гуандун потребовала исправить 215 приложений, нарушающих права пользователей.

22 февраля Управление связи провинции Гуандун уведомило 215 приложений, требующих исправления. Типы приложений можно разделить на 13 категорий, включая игры, покупки, социальные сети, управление финансами и т. Д. Из 215 приложений 116 имеют проблемы с кибербезопасностью. Нарушение прав и интересов пользователей включает: (1) неспособность указать цель, метод и объем личной информации, собираемой и используемой сторонним SDK, интегрированным приложениями в политику конфиденциальности; (2) предварительная подача заявки на разрешение терминала до того, как пользователь прочитает и согласится с политикой конфиденциальности; (3) предварительная подача заявки на открытие адресной книги, местоположения, SMS, записи, камеры, когда пользователи не используют соответствующие функции или услуги;

4. Два финансовых учреждения оштрафованы за незаконную обработку личной информации.

2 февраля, согласно форме информации об административных штрафах, опубликованной отделом управления бизнесом PBC, компания Beijing Guoxu Small Loan Co., Ltd. была оштрафована на 160 000 юаней за разглашение личной информации без уведомления субъекта данных.. Кроме того, Xinhan Bank (China) Co., Ltd. был оштрафован на 570 000 юаней за запрос личной кредитной информации без согласия, а соответствующее ответственное лицо также было оштрафовано на 114 000 юаней.

5. Филиал ICBC в Ляочэн был оштрафован на 36 000 юаней за нарушение данных.

18 февраля, согласно сообщению отделения PBC Liaocheng, отделение ICBC в Liaocheng было оштрафовано на 36 000 юаней за запрос личной информации без согласия субъекта данных. Ван Хунцин, генеральный директор центра банковских карт, ответственное лицо, также был оштрафован на 8000 юаней.

6. Отделение Банка Китая в Ляонине было оштрафовано за неспособность собирать и использовать личную финансовую информацию потребителей в соответствии с требованиями.

3 февраля информация об административных штрафах, опубликованная Шэньянским отделением PBC, показала, что отделение Банка Китая в Ляонин, имевшее пять пунктов обвинения в нарушении защиты данных, было оштрафовано на 1,147 миллиона юаней.. Нарушения включали, среди прочего, отказ от сбора и использования личной финансовой информации потребителей по мере необходимости.

7. Qianbao Pay была наказана за несохранение информации, удостоверяющей личность клиента, в соответствии с требованиями.

24 февраля, согласно форме публикации информации об административных штрафах, опубликованной Департаментом управления бизнесом Чунцина PBC, компания Chongqing Qianbao Technology Service Co., Ltd., у которой было 10 пунктов нарушения защиты данных, была оштрафована на 8,68 миллиона юаней. Эти нарушения включали неспособность хранить необходимую информацию, удостоверяющую личность клиента. Заместитель генерального директора компании и главный специалист по комплаенсу, а также другие пять соответствующих лиц также были оштрафованы совместно - от предупреждения до штрафа в размере от 50 000 до 135 000 юаней. Нарушения компанией в области защиты личной информации и безопасности данных, связанных с ними, в процессе обеспечения согласованности информации о транзакции во всем процессе оплаты, они не выполнили обязательства по идентификации клиента и не сохранили необходимую личность клиента.

8. Маймай был признан виновным в отправке текстовых сообщений незарегистрированным пользователям.

7 февраля Пекинский районный суд Хайдянь объявил решение о нарушении Маймаем конфиденциальности данных. Вкратце, было обнаружено, что веб-сайт Maimai, управляемый Beijing Taoyou Tianxia Technology Development Co., Ltd., отправлял пользователям текстовые сообщения от имени друга без разрешения пользователя. Он раскрыл настоящее имя пользователя и включил сообщение о том, что некоторые бывшие коллеги опознали пользователя, и многие друзья ждут, когда они присоединятся по ссылке. Когда пользователь щелкает ссылку, веб-страница направит их на страницу регистрации Maimai's. Веб-сайт. Впоследствии пользователь предъявил иск Маймаю в суде, требуя конкретных действий, в том числе прекращения нарушения его конфиденциальности веб-сайтом, безвозвратного удаления его личной информации и публикации заявления с извинениями в China Consumer News. Окружной суд Пекина Хайдянь установил, что действиями ответчика незаконным образом была получена и сохранена личная информация истца, такая как контактная информация мобильного телефона, личная информация друга истца и резюме. Кроме того, Maimai без согласия отправлял истцу незапрошенные сообщения с целью получения коммерческой выгоды, что нарушило право истца на мир и неприкосновенность частной жизни. Судебным решением удовлетворены все требования истца.

Развитие отрасли

1. Национальный технический комитет по стандартизации информационной безопасности опубликовал основные направления действий на 2021 год.

25 февраля Национальный технический комитет по стандартизации информационной безопасности опубликовал основные направления действий на 2021 год, охватывающие семь категорий, в том числе акцент на неотложной необходимости работы по обеспечению национальной сетевой безопасности и повышение эффективности предоставления стандартов. В документе указывается, что он будет и дальше разрабатывать национальные стандарты сетевой безопасности в областях промышленного Интернета, блокчейна, искусственного интеллекта и алгоритмов, Интернета вещей и цифровой валюты, готовить официальные документы или отчеты об исследованиях по стандартизации сетевой безопасности, такой как безопасность 5G, таланты в области безопасности распознавания лиц и сетевой безопасности, а также практические рекомендации по классификации и классификации данных и безопасности совместного использования данных.

2. Национальная фондовая биржа и котировочная компания приняла участие в 11-м совместных учениях по чрезвычайным ситуациям по сетевой безопасности.

27 февраля, согласно циркуляру Комиссии по регулированию ценных бумаг Китая об 11-м совместных учениях по чрезвычайным ситуациям по сетевой безопасности ценных бумаг и фьючерсной индустрии, Национальная биржа ценных бумаг и котировочная компания участвовали в совместных учениях по чрезвычайным ситуациям по сетевой безопасности. Среди других участников были China Securities Депозитарий и Клиринговая Корпорация Limited, Shenzhen Securities Communication Co., Ltd., China Securities Index Co., Ltd. и другие принимающие компании, работающие с ценными бумагами…» ***(Mark Robinson, Nanda Lau, James Gong. China – Cyber security and data protection April round up // Herbert Smith Freehills (https://hsfnotes.com/data/2021/04/12/china-cyber-security-and-data-protection-april-round-up/#page=1). 12.04.2021).***

***

Російська Федерація та країни ЄАЕС

«Специализирующаяся на кибербезопасности российская компания Positive Technologies выступила с заявлением в связи с попаданием под санкции США.

«Мы, как компания, отвергаем безосновательные обвинения, выдвинутые в наш адрес министерством финансов США: за почти двадцатилетнюю историю нашей работы нет ни одного факта использования результатов исследовательской деятельности Positive Technologies вне традиций этичного обмена информацией с профессиональным ИБ-сообществом и прозрачного ведения бизнеса.

Наша глобальная цель состоит в создании продуктов и технологий, призванных повышать общую киберзащищенность в масштабах всего мира, а также — в формировании условий для наиболее эффективного противодействия кибератакам в интересах общества, бизнеса и государства вне привязки к геополитике, с максимальной открытостью и ориентированностью на сотрудничество (в том числе международное).

Технологии Positive Technologies используются по всему миру, и сегодня нам доверяют свою безопасность тысячи компаний различных секторов бизнеса и государственные учреждения разных стран. В компании более 1,1 тыс. сотрудников, по итогам 2020 г. мы заработали 5,6 млрд руб. ($73 млн, по РСБУ) и выросли на 55% по отношению к 2019 г. За последние пять лет средний рост компании составил 41%. Независимые международные аналитические агентства неоднократно отмечали нас в числе наиболее быстрорастущих и визионерских компаний в области решений по безопасности и управлению уязвимостями.

Несмотря на то, что компания не является публичной, рынок высоко оценивает нашу капитализацию, видя ее в пределах нескольких миллиардов долларов. Это доказывает высокий интерес к нашим технологиям и серьезный уровень доверия к компании. Для поддержания этого доверия мы придерживаемся принципов максимальной открытости на всех уровнях своей деятельности: от исследовательской до коммерческой, включая финансовую отчетность компании.

Мы известны мировому кибербез-сообществу как визионеры и лидеры в области этичного исследования проблем безопасности. Так, к примеру, наши исследователи выявляют сотни уязвимостей нулевого дня в год в ИТ-системах различных классов и типов. Все найденные уязвимости без исключения предоставляются производителям ПО в рамках политики ответственного разглашения (responsible disclosure) и не подвергаются огласке до тех пор, пока ими не будет выпущено соответствующее обновление. Каждое такое исследование получает высокую оценку со стороны производителей этих систем и используется для повышения защищенности их конечного продукта.

Традиции прозрачности и открытости находят свое отражение и в рамках форума Positive Hack Days, который мы проводим с 2011 г. Форум является публичной площадкой для обмена экспертизой, обучения и повышения квалификации в области кибербезопасности и ежегодно собирает тысячи экспертов в области кибербезопасности и бизнеса разных стран, представителей CTF-движения, ученых, студентов и даже школьников. В связи с пандемией мы перешли в гибридный формат, и поэтому все происходящее на форуме может видеть широкая аудитория в онлайне, где мы обеспечиваем синхронный перевод на английский язык для того, чтобы любой желающий из любой точки мира мог посмотреть интересную ему тему. Мероприятие полностью открыто для посещения и участия.

Мы искренне считаем, что геополитика не должна являться преградой технологическому развитию общества, и со своей стороны продолжим делать то, что у нас хорошо получается — обеспечивать кибербезопасность и повышать киберзащищенность во всем мире. Поэтому мы продолжаем свою работу в штатном режиме с полным соблюдением всех обязательств перед нашими клиентами, партнерами и сотрудниками». ***(Positive Technologies выступила с заявлением по санкциям США // CNews (https://www.cnews.ru/news/line/2021-04-16_positive_technologies_vystupila_s_zayavleniem). 16.04.2021).***

***

«В отчете Sophos «Будущее кибербезопасности в Азиатско-Тихоокеанском регионе и Японии» установлено, что в Малайзии существует пробел в навыках кибербезопасности: почти 60% малазийских предприятий согласны с тем, что отсутствие у их компаний навыков кибербезопасности является проблемой для их организации, и почти 50% согласны с этим. в их организации нет команды, которая могла бы должным образом обнаруживать, расследовать и реагировать на инциденты безопасности.

Однако привлечение квалифицированных специалистов в области кибербезопасности для восполнения этого пробела остается проблемой. Отсутствие подходящего персонала и бюджетные ограничения по-прежнему мешают организациям получать необходимые им навыки внутри компании. 68 процентов компаний в Малайзии борются с набором кандидатов с необходимыми навыками.

Из-за отсутствия талантов в области кибербезопасности и недостаточного бюджета во многих малазийских компаниях эта болевая точка может быть лазейкой, которая открывает двери для кибератак.

Как мировой лидер в области безопасности сетей и конечных точек, Sophos рекомендует компаниям рассмотреть возможность использования управляемой службы реагирования на угрозы, чтобы восполнить пробел, оставленный нехваткой персонала службы безопасности.

Sophos Managed Threat Response (CCO) является полностью управляемым 24/7 угрозы охоты, обнаружение и обслуживание ответа выступил с экспертной группой охотников угрозы. Эта круглосуточная служба может быстро выявлять и нейтрализовать изощренные и сложные киберугрозы, которые в противном случае могли бы остаться незамеченными. Инновационная услуга объединяет машинное обучение с человеческим анализом для развитого подхода к проактивной защите безопасности, помогая небольшим ИТ-командам опережать атаки, потому что ни одна компания, независимо от размера, не застрахована от кибератак.

Быстро растущие возможности подключения и ускоряющиеся темпы цифровой трансформации подвергают Малайзию все более злонамеренной кибер-деятельности. С их постоянно развивающейся природой киберугрозы продолжают становиться все более умными и коварными, что затрудняет борьбу с ними. Вдобавок ко всему, очень немногие организации обладают необходимыми инструментами, людьми и процессами для эффективного управления своей программой кибербезопасности в любое время суток для проактивной защиты от новых и возникающих угроз.

«Организации, у которых есть наиболее успешные программы кибербезопасности, имеют это, потому что они выбирают лучших людей и используют лучшие инструменты. Управляемые сервисы, которые не реагируют на угрозы, в основном бесполезны. Остановка при уведомлении об угрозе не решает проблему, потому что киберпреступники этого не делают. Жду, пока вы их не догоните. Sophos MTR объединяет нашу лучшую в отрасли защиту конечных точек и интеллектуальный EDR с командой экспертов мирового класса по кибербезопасности. Это может помочь решить множество текущих проблем в

области кибербезопасности, в том числе озабоченность по поводу нехватки кадров., ограниченные бюджеты на безопасность и растущие киберугрозы, - сказал Вонг Джун Хунг, региональный менеджер Sophos Malaysia.

При поддержке элитной команды охотников за угрозами и экспертов по реагированию компании могут положиться на Sophos MTR в принятии мер от их имени.

Поскольку малые и средние предприятия составляют 98,5% предприятий Малайзии, для них важно понимать, насколько серьезной может быть кибератака и что всем предприятиям необходима защита от этих угроз на уровне предприятия. Фактически, количество локальных инцидентов, связанных с кибератаками, увеличилось на 109 процентов после вспышки COVID-19, при этом 44% малазийских организаций заявили, что они стали жертвами успешной кибербезопасной атаки за последние 12 месяцев, и почти 50 процентов опрошенных организаций пострадали. От 1 до 10 приступов в неделю. В это число входят организации любого размера, что еще раз свидетельствует о том, что любой бизнес потенциально может стать жертвой киберпреступников.

«Многие малые предприятия не думают, что кибербезопасность стоит вложений - пока не станет слишком поздно и данные их клиентов уже не будут скомпрометированы. Мы понимаем уникальные проблемы, с которыми сталкиваются небольшие компании, поэтому Sophos MTR предлагает гибкие и масштабируемые цены - это простая цена за пользователя и за сервер без каких-либо скрытых дополнительных услуг. Владельцы бизнеса могут масштабироваться по мере роста, что дает им полный контроль над своим бюджетом », - добавил Вонг.

Хотя Sophos MTR является проактивным и почти полностью автоматизированным, он по-прежнему позволяет клиентам полностью контролировать решения для следующих шагов. Это означает, что пользователь контролирует, как и когда обостряются потенциальные инциденты, какие реакции они хотят предпринять и кого следует включать в уведомления…» ***(Wong Joon Hoong. Bridging the cybersecurity skills gap in Malaysia // The Edge Communications Sdn. Bhd. (https://www.theedgemarkets.com/content/advertise/bridging-cybersecurity-skills-gap-malaysia). 14.04.2021).***

***

«Правительство штата Виктория планирует инвестировать в общей сложности 30 миллионов австралийских долларов в обновление и модернизацию ИТ-инфраструктуры 28 больниц и служб здравоохранения штата, чтобы защититься от дальнейших кибератак.

30 миллионов австралийских долларов будут распределены между больницами Мельбурна и региональными и сельскими службами здравоохранения. Больницы Мельбурна получат большую часть почти 22 миллиона австралийских долларов, а оставшиеся 8 миллионов австралийских долларов будут разделены между региональными и сельскими службами здравоохранения.

Финансирование, которое будет предоставлено в рамках программы обновления клинических технологий правительства штата, будет использовано

специально для замены старых серверов и операционных систем новой инфраструктурой.

Правительство штата заявило, что новая инфраструктура сократит сбои ИТ, повысит скорость сети, поддержит развертывание Wi-Fi у постели пациентов, а также обеспечит загрузку и просмотр медицинских изображений с высоким разрешением, телемедицину и доступ к клинической поддержке. и патология возникает из других больниц.

«Мы помогаем больницам и службам здравоохранения штата Виктория модернизировать компьютеры и ИТ-инфраструктуру для повышения надежности и кибербезопасности», - сказал министр здравоохранения Виктории Мартин Фоули. «Речь идет о защите наших служб здравоохранения от кибератак».

В прошлом месяце хирургические операции, проводимые Eastern Health в Виктории, были вынуждены отменить некоторые посещения пациентов после «киберинцидента».

Eastern Health управляет больницами Angliss, Box Hill, Healesville и Maroondah, а также управляет многими другими учреждениями.

В своем заявлении Eastern Health сообщила, что в ответ на инцидент отключила многие из своих систем.

«Многие ИТ-системы Eastern Health были отключены в качестве меры предосторожности, пока мы стремимся разобраться и исправить ситуацию», - говорится в сообщении.

«Важно отметить, что безопасность пациентов не была поставлена под угрозу».

Еще в 2019 году подобный инцидент произошел в больницах Виктории, в результате чего они отключились от Интернета в попытке изолировать заражение от программ-вымогателей.

В то время Управление премьер-министра и Кабинет министров штата Виктория сообщило, что пострадавшие больницы входили в Альянс здравоохранения Гиппсленда и Юго-западный альянс сельского здравоохранения.

Инцидент произошел вскоре после того, как Управление генерального аудитора штата Виктория (VAGO) охарактеризовало систему общественного здравоохранения штата как крайне уязвимую для кибератак, и в отчете отмечалось, что слабые места в области безопасности в собственном технологическом подразделении Министерства здравоохранения и социальных служб (DHHS) являются повышение вероятности нарушения в 61% государственных медицинских услуг.

«Есть ключевые слабые места в физической безопасности медицинских служб и в их логической безопасности, которая охватывает управление паролями и другие средства контроля доступа пользователей», - пишет VAGO. «Осведомленность персонала о безопасности данных низкая, что увеличивает вероятность успеха таких методов социальной инженерии, как фишинг или проникновение в корпоративные зоны, где могут быть расположены инфраструктура и серверы ИКТ».

В ходе аудита VAGO исследовал трех поставщиков медицинских услуг - Barwon Health, Королевскую детскую больницу и Королевскую викторианскую

больницу для глаз и ушей - и изучил, как две разные области DHHS - отделение цифрового здравоохранения и решение для медицинских технологий - предоставлять медицинские услуги в штате.

Изучая службы здравоохранения, VAGO заявила, что также может получить доступ к учетным записям, в том числе административным, с помощью «основных хакерских инструментов». У учетных записей были слабые пароли и не было MFA.

«Все проверенные службы здравоохранения должны делать больше для защиты данных о пациентах», - говорится в отчете. «Мы также обнаружили, что службы здравоохранения не имеют надлежащих структур управления и политики для поддержки безопасности данных». ***(Aimee Chanthadavong. Victorian government earmarks AU$30m to lift hospital cyber capabilities // ZDNet (https://www.zdnet.com/article/victorian-government-earmarks-au30m-to-lift-hospital-cyber-capabilities/). 15.04.2021).***

***

«Федеральное правительство Австралии, возможно, наконец откажется от своей мантры «каждое агентство за себя, когда дело доходит до кибербезопасности », сигнализируя в среду о своем намерении заставить более крупные агентства Канберры оказывать поддержку другим.

«Мы знаем, что определенные агентства не могут конкурировать за навыки и ресурсы на рынке, и мы должны разработать альтернативные способы удовлетворения их потребностей», - сказал министр занятости, трудовых ресурсов, навыков, малого и семейного бизнеса Стюарт Роберт.

Бывший министр государственных услуг показал, что правительство рассчитывает создать три пилота «Cyber Hub», которые будут видеть отделы, такие как обороны, внутренних дел и служб Австралии предоставляют кибер - услуги для «тех учреждений, которые не могут соответствовать их широту и глубину навыков».

«Мы можем видеть будущее, в котором такие модели концентраторов могут быть созданы для других типов масштабируемых услуг, а не только для кибербезопасности», - сказал он. «Это может включать более широкие функции ИКТ, такие как защищенная электронная почта, или корпоративные услуги, такие как финансы или управление персоналом».

Решения будут проинформированы Общегосударственной архитектурой и Цифровым обзором, которые являются проектами, реализуемыми Агентством цифровой трансформации (DTA).

DTA, которое теперь снова находится в ведении Департамента премьер-министра и Кабинета министров и с пересмотренным мандатом, отвечающим за «общегосударственное управление, стратегию, политику, архитектуру, процессы и процедуры ИКТ в правительстве», собирается предоставить Роберту «полный картина того, что у нас есть, что нам нужно, во что мы должны инвестировать и когда» в рамках создания целостной правительственной архитектуры.

«Я поручил DTA разработать целостную правительственную архитектуру, которая будет отображать все стратегические возможности, необходимые нам как

правительству, включая существующие активы и любые пробелы, которые нам необходимо устранить», - сказал он.

«Архитектура также будет учитывать возраст и сложность существующих систем и позволит нам начать управлять жизненным циклом проектов».

Точно так же DTA проводит цифровой обзор, который, по словам Роберта, дает правительству четкое представление о возможностях агентств, например о том, какие уровни квалификации существуют, на каком уровне зрелости и как различные агентства в настоящее время выполняют свои функции. их ролей.

"После завершения в предстоящий период у нас будет возможность объединить системное представление всей правительственной архитектуры и представление возможностей агентства в Digital Review, чтобы понять, как мы начинаем планировать будущее в масштабе предприятия во всем правительстве или вся нация», - считает Роберт.

Между тем, по его словам, «комплексный инвестиционный подход» позволит правительству принимать правильные инвестиционные решения.

«Прямо сейчас инвестиции в цифровые и ИКТ могут быть чем-то вроде голодных игр, когда правительство часто сталкивается с инвестиционными предложениями, которые представляются как срочные или критические, но с ограниченными возможностями для рассмотрения более широкого стратегического контекста этих предложений», - сказал он.

Роберт также воспользовался возможностью, чтобы осветить свое видение myGov, онлайн-портала федерального правительства для доступа к государственным услугам.

«Наше долгосрочное видение myGov - обеспечить его развитие и превращение в ведущую в мире единую национальную цифровую платформу, которая предоставляет простые, полезные, уважительные и прозрачные услуги, отвечающие потребностям и ожиданиям всех австралийцев», - сказал он, отдавая дань уважения эту неповторимую мечту он передал Национальному пресс-клубу в июле.

«Мы будем постепенно предоставлять новые функции, предоставлять персонализированную информацию и услуги, поскольку мы стремимся к еще более интегрированному и улучшенному обслуживанию клиентов.

«Мы строим будущее правительство - открыто и прозрачно».

В марте прошлого года myGov потерпел крах, когда многие австралийцы пытались определить, имеют ли они право на поддержку по схеме Centrelink страны.

Роберт поспешил заявить, что портал подвергся распределенной атаке типа «отказ в обслуживании» (DDoS), одновременно обвинив в отключении легитимный трафик, который превысил установленный правительством предел в 55 000 одновременных пользователей.

Технически подкованный министр также воспользовался возможностью, чтобы выделить свои «большие, волосатые, дерзкие цели» - или «B-HAGs», как заявили его спичрайтеры.

«Правительство, особенно федеральное правительство, предоставляет огромные средства австралийцам, но большая их часть находится под капотом, а большая часть основана на технологиях», - сказал Роберт.

«И это совсем не «сексуально».

«Работа меня и моих коллег - не сделать правительство «сексуальным», а сделать государственные услуги простыми, полезными, уважительными и прозрачными».

Роберт коснулся Стратегии цифровой трансформации, цель которой - сделать все государственные услуги доступными в цифровом виде к 2025 году. Он сказал, что "значительный прогресс как в доставке, так и в наших возможностях и зрелости" был достигнут по мере приближения половины пути». ***(Asha Barbaschow. Australian government's major IT shops to help others with cybersecurity // ZDNet (https://www.zdnet.com/article/australian-governments-major-it-shops-to-help-others-with-cybersecurity/). 28.04.2021).***

***

«Комиссар Австралии по электронной безопасности собирается получить широкие новые полномочия, такие как возможность отдавать приказ об удалении материалов, которые серьезно вредит взрослым, с приближающимся принятием Закона о безопасности в Интернете.

Технологические фирмы, а также эксперты и группы по защите гражданских свобод оспорили Закон, например, из-за его поспешного характера, вреда, который он может нанести индустрии для взрослых, и властных полномочий, которые он наделяет электронной безопасностью, например. Нынешний комиссар по электронной безопасности Джули Инман Грант даже ранее признавала, что детали того, как будут контролироваться меры, предусмотренные в Законе о онлайн-безопасности 2021 года, все еще прорабатываются.

Законопроект содержит шесть приоритетных областей, включая схему киберпреступлений среди взрослых, направленную на удаление материалов, наносящих серьезный вред взрослым; схема злоупотреблений на основе изображений для удаления интимных изображений, которые были переданы без согласия; Основные ожидания безопасности в Интернете (BOSE) для уполномоченного по электронной безопасности для обеспечения подотчетности служб; и схема онлайн-контента для удаления «вредных» материалов с помощью полномочий на удаление.

Выступая перед Объединенным парламентским комитетом по разведке и безопасности в рамках его расследования экстремистских движений и радикализма в Австралии, Инман Грант сказала, что, несмотря на то, что порог новых полномочий довольно высок в отношении запросов на уничтожение, это даст ее агентству изрядную сумму. у вас есть возможность взглянуть на пересекающиеся факторы, такие как намерение поста.

«Я думаю, что язык преднамеренно - он ограничен таким образом, чтобы дать нам некоторую свободу... мы должны смотреть на мессенджера, мы должны смотреть на сообщение, и мы должны смотреть на цель», - она сказал в четверг.

Закон также не будет применяться к группам людей, а скорее к отдельным лицам. Комиссар предположил, что это произошло из-за соблюдения баланса свободы слова.

«Я думаю, что наделение нас более широким набором полномочий для массового нападения на группу или цель, вероятно, вызовет гораздо больше вопросов о правах человека», - сказала она.

Она сказала, что это случай «написания сценария» по мере того, как он разворачивается, учитывая, что на международном уровне нет аналогичного закона, который бы помогал руководствоваться этим законом. Инман Грант сказала, что она пыталась внушить ожидания, что не собирается вести «крупномасштабную скорострельную стрельбу».

«Поскольку каждое отдельное уведомление об удалении или меры по исправлению положения, которые мы принимаем, должны будут предстать перед судом, они должны выдержать проверку со стороны AAT, омбудсмена и других», - сказала она. «Таким образом, порог высок, он действительно, вероятно, будет нацелен на худшие из худших с точки зрения целенаправленных злоупотреблений в Интернете».

Комиссара беспокоит то, что платформы социальных сетей имеют широкий доступ ко всем видам сигналов, которые происходят на их платформах, но они часто вмешиваются, когда уже слишком поздно.

«Я думаю, что то, что мы видели с осадой Капитолийского холма, это то, что на самом деле только к 11-му часу они последовательно проводили в жизнь свою собственную политику», - сказала она. «Так что я думаю, что мы видели реальное избирательное применение некоторых из этих политик, и нам нужно добиться большей последовательности».

ИЗБЕЖАНИЕ МОЛОДЫ

Она считает, что BOSE каким-то образом исправит это. Не устанавливая этих ожиданий, Инман Грант сказала, что будет пытаться вдохновить свою команду, чтобы «сыграть в большую игру «вонзай крота».

Обнаружив одних и тех же преступников, использующих один и тот же образ действий для нападения на других, Инман Грант сказал, что это яркий пример того, где безопасность по замыслу так важна.

«Вы строите цифровые дороги, где ваши ограждения, где ваши встроенные ремни безопасности и что вы делаете, чтобы принимать сигналы?», - сказала она.

"Меня не волнует, что это такое, используете ли вы обработку естественного языка, чтобы посмотреть на общий язык, который может быть использован, или на IP-адреса, есть ряд сигналов, которые они могут - они должны относиться к этому как к оружию. расы, они должны играть в игру «бей крота», а не в жертву и регулирующие органы».

Инициатива «Безопасность благодаря конструкции» стартовала в 2018 году с основных платформ. В настоящее время в рамках инициативы eSafety участвует около 180 различных технологических компаний и активистов.

Инман Грант назвал это «проблемой культурных изменений», то есть изменение общеотраслевого этоса, согласно которому быстрое движение и ломка вещей приносят результаты.

«Как нам перестать нас всех ломать?» - спросила она. «Потому что вы так быстро переходите к следующей функции, к следующему продукту, что не оцениваете риски заранее и не создаете средства защиты на начальном этапе.

«Я имею в виду, сколько раз мы должны видеть момент технической катастрофы, когда компании - даже начинающие компании - должны знать лучше».

Решение, по ее словам, заключается не в том, чтобы правительство предписывало исправления технологий, а в том, чтобы усилить обязанность проявлять осторожность, когда компании делают что-то неправильно, например, с помощью таких инициатив, как безопасность по замыслу. Инман Грант сказал, что BOSE в определенной степени повысит уровень прозрачности.

«Мы призываем их к ответу за злоупотребления, которые происходят на их платформах, мы выступаем в качестве подстраховки, когда что-то выходит из строя, и мы говорим им, чтобы они это прекратили», - сказала она. «Платформы - это посредники... платформы [позволяют] этому случиться, но в основном мы говорим о человеческом поведении, человеческих преступлениях, преступных действиях в Интернете, направленных против людей».

Инман Грант сказал, что eSafety в настоящее время работает с венчурным капиталом и сообществом инвесторов, «потому что они часто взрослые в комнате», над разработкой интерактивного инструмента оценки безопасности путем проектирования, одного для стартапов, а другого для средних и крупных компаний. это должно быть обнародовано в течение следующих трех недель.

КАК РЕАЛЬНЫЙ МИР, ПРОСТО ЦИФРОВОЙ

«Прошло всего 50 лет с тех пор, как в автомобилях потребовались ремни безопасности, и это вызвало много возражений. Теперь они руководствуются международными стандартами. Мы говорим о стандартной ответственности за качество продукции - вам не разрешается производить товары, которые могут причинить вред. люди, согласно стандартам безопасности пищевых продуктов вам не разрешается травить людей или делать их больными - это не должны быть стандарты или требования, которых технологические компании должны избегать», - сказал комиссар.

«Интернет стал важной полезностью... им тоже нужно жить по этим правилам. И если они не собираются делать это добровольно, то у них будет лоскутное одеяло из законов и постановлений, потому что правительства будут регулировать их по-разному».

Инман Грант сказал, что eSafety взаимодействует с платформами социальных сетей каждый день и добился 85% успеха при удалении изображений и видео интимного характера, которые не были согласованы.

«Обычно это то, что мы называем «мошенническими порносайтами», которые не поддаются уничтожению», - сказал Инман Грант. «И, конечно же, мы видим много общего в том, что касается хостинговых услуг и типов сайтов, на которых размещаются сети педофилов, а также про террористический или кровавый контент».

По ее словам, в eSafety наблюдался всплеск всех форм онлайн-злоупотреблений за период COVID, но это было не по той причине, по которой многие думали.

«Мы часто говорим о том, что наблюдаем много случаев сексуального насилия над детьми в даркнете, но мы видели намного больше в открытой сети и в открытых местах, таких как Twitter, Instagram и Facebook - в некоторых случаях до 650%. по сравнению с прошлым годом ", - сказала она.

"Это было не просто упрощенное объяснение того, что все больше детей были в сети без присмотра [и было больше] хищников, нацеленных на них, что, безусловно, произошло, но на самом деле происходило то, что многие компании передали свои услуги модерации контента третьим лицам, и многие из них находятся на Филиппинах и в Румынии, в развивающихся странах, где эти работники были отправлены домой и не могли просматривать контент».

Она сказала, что из-за того, что персонал по модерации контента не может просматривать контент, и преобладание большего количества людей в сети, создали «идеальный шторм».

«Вы видели, как некоторые компании используют больше искусственного интеллекта и аналитических инструментов, но они все еще очень несовершенны. И почти все платформы, которые действительно используют инструменты искусственного интеллекта, всегда используют часть человеческой модерации, потому что это просто не на должном уровне». ***(Asha Barbaschow. Australia's eSafety and the uphill battle of regulating the ever-changing online realm // ZDNet (https://www.zdnet.com/article/australias-esafety-and-the-uphill-battle-of-regulating-the-ever-changing-online-realm/). 30.04.2021).***

***

«Австралия решила, что шестилетним детям необходимо образование по вопросам кибербезопасности, даже несмотря на то, что это исключило другие материалы из национальной учебной программы.

В недавно представленный недавно пересмотренный проект национальной учебной программы для детей в возрасте от пяти до шестнадцати лет был добавлен новый раздел под названием «Учет конфиденциальности и безопасности», который «предполагает, что учащиеся разрабатывают соответствующие методы управления личными данными и эффективно внедряют протоколы безопасности.»

Предлагаемая учебная программа направлена на то, чтобы научить пятилетних детей - возраста, в котором австралийские дети впервые посещают школу - не делиться информацией, такой как дата рождения или полные имена, с незнакомцами, и что они должны проконсультироваться с родителями или опекунами перед вводом личной информации. онлайн.

Детей шести и семи лет научат использовать имена пользователей и пароли, а также научат ловушкам нажатия всплывающих ссылок на соревнования.

К тому времени, когда дети пойдут в третий и четвертый классы, их научат определять личные данные, которые могут храниться в онлайн-сервисах, и как они могут раскрыть их местонахождение или личность. Учителя также обсудят «использование псевдонимов и почему они важны при игре в онлайн-игры».

К концу начальной школы детей научат уважительно относиться к Интернету, в том числе «уважительно реагировать на мнение других людей, даже если оно отличается от личного мнения».

В новой учебной программе сохранено решение Австралии от 2015 года распространить цифровые технологии на другие предметы, решение, которое было принято, несмотря на то, что в ранних проектах предусматривалось создание классов, посвященных программированию. Такие классы были исключены, потому что учителям не хватало навыков, а у школ не было ресурсов, чтобы принять план.

В новом проекте учебной программы удалено около 20 процентов материала, что является ответом на обвинения в том, что нынешняя учебная программа «переполнена». Поэтому примечательным является предложение кибер-навыков в качестве дополнения, хотя они могут не пережить процесс консультаций, также начатый вчера.

Национальная учебная программа Австралии разрабатывается федеральным правительством, у которого нет школ. Правительства штатов и территорий получают эту работу и, что является великолепным примером бюрократической эффективности, могут выбрать использование национальной учебной программы или разработать свою собственную». ***(Simon Sharwood. Australia proposes teaching cyber-security to five-year-old kids // The Register (https://www.theregister.com/2021/04/30/eaching_cybersecurity_to_five_year_olds/). 30.04.2021).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«15 апреля 2021 года президент Байден издал новое распоряжение о блокировании собственности в отношении определенных вредных видов иностранной деятельности правительства Российской Федерации (далее - «ЕО»). ЕО не налагает общих ограничений на торговлю с участием США и России, а вместо этого применяет более адресный подход. В частности, ЕО вводит новые санкции в отношении оборонного и технологического секторов российской экономики, запрещает финансовым учреждениям США совершать первичные операции с новым российским суверенным долгом и сопровождается рядом обозначений физических и юридических лиц в России как «специально предназначенных для США». Граждане подлежат санкциям.

Секторальные и вторичные санкции

ЕО определяет несколько действий, которые теперь могут привести к наложению блокирующих санкций. ЕО обычно делегирует право наложения санкций Министерству финансов и Государственному департаменту, за некоторыми исключениями (указанными ниже). Это продолжает недавнюю тенденцию делегирования ответственности за санкции другим ведомствам в дополнение к OFAC или совместно с ним. Новые основания для назначения санкций включают:

«Работа» в технологическом или оборонном секторах российской экономики: ЕО разрешает блокирующие санкции в отношении лиц, определенных «для работы или работавших в технологическом секторе или в оборонном и связанном с

материальными [sic] секторе экономики Российской Федерации». «Сектор технологий» и «сектор оборонных и связанных с ним материалов» не определены ни в ЕО, ни в текущих инструкциях OFAC или Госдепартамента, и поэтому могут охватывать широкий спектр деятельности (включая инвестиции) в российский технологический и оборонный секторы. Обратите внимание, что связанные с обороной организации SSI, указанные в соответствии с Директивой 3 ЕО 13662, не подпадают под запреты в соответствии с новым ЕО, если они не наложены на них конкретно санкциями в соответствии с ЕО. (Часто задаваемые вопросы OFAC 887.)

Могут быть названы дополнительные секторы экономики: ЕО также уполномочивает министра финансов (по согласованию с государственным секретарем) определять дополнительные секторы экономики Российской Федерации, которые могут повлечь за собой блокирующие санкции.

Нарушение поставок газа или энергии в Европу, Кавказ или Азию: ЕО разрешает блокирующие санкции в отношении лиц, признанных ответственными за или соучастниками, либо прямо или косвенно участвовавших или пытавшихся участвовать, отключая или нарушая газовые или поставки энергии в Европу, Кавказ или Азию, и быть: (i) гражданином или гражданином России; или (ii) организация, учрежденная в соответствии с законодательством России или российской юрисдикции (включая иностранные филиалы). Термины «резка или разрушение» не определены.

Вмешательство в выборы, кибератаки и коррупционная деятельность: ЕО санкционирует блокирующие санкции в отношении лиц, которые, как установлено, участвовали в широком спектре действий, связанных с вмешательством в выборы, кибератаками и коррупцией. В целом, действия включают: (i) злонамеренные кибер-действия; (ii) вмешательство правительства США или другого иностранного государства в выборы; (iii) вмешательство в демократические процессы в США и за рубежом; (iv) транснациональная коррупция; (v) физический ущерб лицам или гражданам США или гражданам союзников и партнеров США; (vi) действия, подрывающие мир, безопасность, политическую стабильность или территориальную целостность США, их союзников или партнеров; или (vii) вводящие в заблуждение или структурированные транзакции или сделки с целью обхода любых санкций США, в том числе посредством использования цифровых валют или активов или использования физических активов.

Санкции правительства России и государственных чиновников: ЕО санкционирует блокирующие санкции в отношении лиц, определенных Государственным департаментом в качестве руководителей, должностных лиц, старших должностных лиц или членов совета директоров российского правительства, организаций, которые участвовали в вмешательстве в выборы, кибератаках и коррупционной деятельности, или лица, заблокированные по ЕО. Точно так же могут быть заблокированы политические подразделения, агентства или органы правительства России, а также супруги или взрослые дети лиц, которые были заблокированы в соответствии с ЕО в качестве должностных лиц российского правительства, или за вмешательство в выборы, кибератаки и коррупционную деятельность. «Правительство Российской Федерации» определяется в широком смысле и включает «Правительство Российской Федерации, любое политическое

подразделение, агентство или их структуру,действует от имени или в интересах Правительства Российской Федерации». (Курсив добавлен.)

Ограничения по суверенному долгу

15 апреля Казначейство также издало « Директиву 1 » в соответствии с ЕО. Директива 1:

определяет Центральный банк, Фонд национального благосостояния и Министерство финансов Российской Федерации как «политические подразделения, агентства или структуры» правительства России (см. выше); а также

запрещает «финансовым учреждениям США»: (i) участие на первичном рынке рублевых или нерублевых облигаций, выпущенных после 14 июня 2021 г. Центральным банком, Фондом национального благосостояния или Министерством финансов; и (ii) кредитование средств в рублях или не в рублях Центральному банку, Фонду национального благосостояния или Министерству финансов.

Согласно Директиве 1, термин «финансовое учреждение США» означает любое юридическое лицо в США (включая его зарубежные отделения), которое занимается бизнесом по приему депозитов, внесению, предоставлению, передаче, хранению или посредничеству ссуд или другим видам предоставления кредита, или покупка или продажа иностранной валюты, ценных бумаг, товарных фьючерсов или опционов или закупка их покупателями и продавцами в качестве принципала или агента. Термин включает депозитарные учреждения, банки, сберегательные банки, трастовые компании, брокеров и дилеров по ценным бумагам, брокеров и дилеров по фьючерсам и опционам, торговцев форвардными контрактами и иностранной валютой, биржи ценных бумаг и товаров, клиринговые корпорации, инвестиционные компании, планы вознаграждения сотрудников и США. холдинговые компании, филиалы в США или дочерние компании в США любого из вышеперечисленного. Этот термин включает в себя те филиалы, офисы,

Директива Закона о химическом и биологическом оружии («ХБО») уже запрещала «банкам США», включая иностранные отделения,: (i) участвовать на первичном рынке нерублевых облигаций, выпущенных российским государством; и (ii) предоставление ссуды нерублевым фондам государству России после 26 августа 2019 г. Запреты в соответствии с Директивой 1 аналогичны ограничениям в соответствии с Директивой Закона о ХБО, за исключением того, что Директива 1 в более широком смысле применяется к: (i) «Финансовые учреждения США »(как определено выше); и (ii) операции с рублевыми и нерублевыми облигациями и фондами. (Часто задаваемые вопросы OFAC 890.)

Обратите внимание, что:

Директива 1 не распространяется на вторичный рынок указанных выше облигаций. (Часто задаваемые вопросы OFAC 889.)

«Правило 50%» OFAC не применяется в соответствии с Директивой 1, т. Е. Ограничения Директивы 1 не применяются к организациям, прямо или косвенно принадлежащим 50% или более Центральному банку, Фонду национального благосостояния или Министерству финансов. (Часто задаваемые вопросы OFAC 891.)

Сопровождающие обозначения

Наряду с новым ЕО, OFAC объявило ряд обозначений физических и юридических лиц в соответствии с новыми полномочиями в ЕО и существующими санкционными положениями США…». ***(Jonathan Cross, Christopher Boyd, Brittany Crosby-Banyai, Christopher Milazzo. Biden Administration Announces New Russia-Related Sanctions in Response to Cybersecurity, Election Interference, Energy Issues // Herbert Smith Freehills (https://hsfnotes.com/sanctions/2021/04/15/biden-administration-announces-new-russia-related-sanctions-in-response-to-cybersecurity-election-interference-energy-issues/#page=1). 15.04.2021).***

***

«В понедельник израильские шпионские агентства обвинили Иран в использовании фальшивых аккаунтов в социальных сетях, чтобы заманить граждан еврейского государства за границей, «чтобы нанести им вред или похитить».

Заявление Израиля прозвучало через несколько часов после того, как Иран обвинил своего заклятого врага в организации атаки на ключевой ядерный объект и пообещал «отомстить».

В заявлении агентства внутренней безопасности Израиля Шин Бет говорится, что оно и международная разведка Моссад раскрыли «метод», с помощью которого «иранские разведчики» использовали фальшивые профили в Instagram женщин, «по-видимому, занимающихся бизнесом и туризмом», для нацеливания на израильтян.

В заявлении говорится, что оперативники будут использовать профили, чтобы обратиться к израильтянам, имеющим международные деловые контакты, и попытаться «вовлечь их в романтические или коммерческие встречи» в странах по всему миру.

Израильские разведывательные организации «искренне обеспокоены» тем, что иранская деятельность «может привести к попыткам причинить вред или похитить израильтян в этих странах», - говорится в сообщении Шин Бет, отметив, что аналогичная тактика была использована Ираном против противников режима в Европе.

Израильский чиновник, выступавший на условиях анонимности, сообщил AFP, что был «по крайней мере один случай, когда гражданин уехал в другую страну для проведения встречи» после того, как связался с подозрительной учетной записью в социальной сети.

«Человек был предупрежден (израильской) разведкой и вернулся (домой)», - сказал чиновник.

Согласно сообщениям, напряженность в отношениях между Ираном и Израилем в последние недели возросла, поскольку противники обмениваются атаками на торговые суда друг друга.

В понедельник Иран заявил, что накануне в центре распределения электроэнергии его завода по обогащению урана в Натанзе произошел «небольшой взрыв», что министерство иностранных дел назвало израильским актом «терроризма».

Израиль выступил против недавно возобновленных переговоров с Ираном при поддержке ЕС, направленных на спасение международного соглашения 2015 года по ядерной программе Тегерана, которое было разорвано с тех пор, как США в одностороннем порядке вышли из этого соглашения в 2018 году.

Израиль считает, что Иран обманывает сделку и работает над созданием ядерного оружия, в то время как Тегеран отрицает такие амбиции». ***(Iran Used Fake Instagram Accounts to Try to Nab Israelis: Spy Agencies // Wired Business Media (https://www.securityweek.com/iran-used-fake-instagram-accounts-try-nab-israelis-spy-agencies). 12.04.2021).***

***

«Официальные лица заявили во вторник, что организация, которая курирует национальные спортивные федерации Швеции, была взломана российской военной разведкой в 2017-2018 годах в ходе кампании по взлому данных, которая также затронула некоторые ведущие спортивные организации мира, включая ФИФА и Всемирное антидопинговое агентство.

Шведские прокуроры заявили, что «неоднократные и всеобъемлющие нарушения» Шведской спортивной конфедерации со стороны ГРУ привели к тому, что к личным данным спортсменов, таким как медицинские записи, был получен доступ, и эта информация была опубликована шведскими СМИ.

Взлом был обнаружен в результате расследования, проведенного Службой безопасности Швеции в сотрудничестве со службами безопасности других стран. Но расследование было прекращено, потому что «отсутствуют необходимые предварительные условия для возбуждения судебного дела за границей или экстрадиции в Швецию», - сказал прокурор Матс Юнгквист.

Утверждается, что утечки данных произошли с декабря 2017 года по май 2018 года. В то время Швеция готовила заявку на проведение зимних Олимпийских игр 2026 года.

Среди спортсменов, получивших доступ к частной информации, была футболистка женской национальной сборной Оливия Шоу.

«Это серьезное преступление против человечности и ценностей, когда личная информация, которая может быть конфиденциальной, была распространена без малейшего размышления о том, как она может повлиять на людей», - сказал Бьорн Эрикссон, председатель Шведской спортивной конфедерации.

Юнгквист сказал, что утечки данных были частью более масштабной систематической кампании российских хакеров против международных спортивных организаций, таких как ФИФА, ВАДА, Антидопинговое агентство США и Спортивный арбитражный суд. В 2018 году Соединенные Штаты предъявили обвинения в предполагаемом взломе Россией олимпийских и футбольных объектов.

Хакерская кампания началась после того, как в 2015 году была раскрыта поддерживаемая государством российская допинговая программа». ***(Swedish Sports Body Hacked by Russians, Officials Say // Wired Business Media (https://www.securityweek.com/swedish-sports-body-hacked-russians-officials-say). 13.04.2021).***

***

«Бизнес все чаще подвергается критике со стороны хакеров, поддерживаемых национальным государством, поскольку правительства по всему миру участвуют в атаках, чтобы украсть секреты или заложить основу для будущих атак.

Национальные государства, киберконфликт и сеть прибыли, исследование, проведенное исследователями кибербезопасности из HP и криминологами из Университета Суррея, предупреждает, что количество ключевых атак на национальные государства значительно выросло за последние три года - и что предприятия и предприятия все чаще становятся мишенью.

Анализ кибератак между национальными государствами в период с 2017 по 2020 год показывает, что чуть более трети организаций, подвергшихся атаке, были предприятиями: киберзащита, СМИ, правительство и критическая инфраструктура также являются частыми целями этих атак, но предприятия поднялись на вершину рейтинга. список.

«Независимо от сектора или размера, бизнес, похоже, теперь сталкивается с сопоставимыми рисками со стороны национальных государств, как и со стороны традиционных киберпреступников», - говорится в исследовательском документе.

Основная цель этих атак - получение интеллектуальной собственности или бизнес-аналитики, причем особому риску подвергаются технологические фирмы и фармацевтические компании.

События прошлого года увеличили риски, потому что не только национальные государства проводят кампании, стремясь получить доступ к исследованиям вакцины COVID-19, но и то, как многие люди работают из дома, оставило их - и их работодателей. - при дополнительном риске фишинга и других атак.

«Национальные государства тратят значительное время и ресурсы на достижение стратегических киберпреимуществ, чтобы продвигать свои национальные интересы, возможности сбора разведывательной информации и военную мощь посредством шпионажа, подрывных действий и воровства», - сказал доктор Майк МакГуайр, старший преподаватель криминологии в Университете им. Суррей.

«Попытки получить данные интеллектуальной собственности о вакцинах и атаки на цепочки поставок программного обеспечения демонстрируют, на что готовы пойти государства для достижения своих стратегических целей».

Хакеры также готовы использовать методы, которые могут подвергнуть риску многие компании, чтобы атаковать несколько.

«Сейчас есть готовность поставить под угрозу тысячи сетей и предприятий, нанеся огромный сопутствующий ущерб, хотя на самом деле истинные цели этих кибератак будут намного меньше», - сказал Ян Пратт, глава отдела безопасности персональных систем в HP Inc.

Чтобы защитить сети от кибератак, в отчете рекомендуется, чтобы организации делали все возможное для защиты конечных точек и сегментации

сетей, чтобы конфиденциальная информация не хранилась в легкодоступных местах, если злоумышленник пытается проникнуть в сеть.

Также рекомендуется, чтобы организации своевременно применяли исправления безопасности, чтобы они были защищены от известных уязвимостей при их возникновении.

«Поскольку масштабы и изощренность атак на национальные государства продолжают расти, организациям жизненно важно инвестировать в безопасность, которая помогает им опережать эти постоянно меняющиеся угрозы», - сказал Пратт». ***(Danny Palmer. Nation-state cyberattacks targeting businesses are on the rise // ZDNet (https://www.zdnet.com/article/nation-state-cyber-attacks-targeting-businesses-are-on-the-rise/). 09.04.2021).***

***

«В конце марта в австралийском парламенте произошел сбой в сфере ИТ, в результате которого депутаты и сенаторы потеряли доступ к электронной почте на выходных, а некоторые в течение недели жаловались на то, что их доступ был «неоднородным».

Перед сенаторами во время слушаний по дополнительным оценкам в среду генерального директора Австралийской разведывательной организации (ASIO) Майка Берджесса спросили об инциденте и о том, получило ли его агентство информацию об этом.

«Нет, мы обычно не получаем информацию об отключении», - ответил он. «Но, конечно, нам поручено рассматривать угрозы безопасности, включая потенциальный шпионаж и иностранное вмешательство, поэтому мы обращаем внимание на действия, и у нас есть понимание того, что там произошло».

Он сказал, что этот инцидент не ему комментировать, предлагая сенаторам направить свои вопросы другим.

Он действительно сказал, что не был обеспокоен этим отключением напрямую.

«Конечно, сейчас полезно подчеркнуть, что шпионаж, в том числе кибершпионаж, жив и здоров», - сказал он. «И будут люди, у которых есть взломы сетей и мобильных устройств, но это не [только] национальные государства, это могут быть преступники или отдельные лица.

«Существует ряд причин, по которым сети могут быть нарушены, но это может быть не из-за кибер-злоумышленников или преступных действий, на самом деле это может быть просто действие, которое сетевые операторы предпринимают для нарушения».

Отказавшись от характеристики, что это было «нападением», Берджесс подтвердил свою позицию.

«Меня как директора службы безопасности не волнует то, что я видел», - повторил он.

«С моей точки зрения, имеет место шпионаж или кибершпионаж?» Меня не беспокоит этот инцидент.

"Конечно, в целом, любая сеть, подключенная к Интернету, часто подвергается этому, и уровни попыток кибершпионажа в этой стране довольно

высоки, поэтому я по-прежнему обеспокоен этим, а также действиями других [австралийских кибершпионажей Центр безопасности], который занимается условиями этого отключения, меня это не касается».

Берджесса также попросили высказать свое мнение о статусе сетей Департамента парламентских служб.

«Мы не занимаемся деталями кибербезопасности», - сказал он.

«Мы больше сосредоточены на реальных угрозах, исходящих от этой страны, в том числе на сетях Департамента парламентских служб, на том, как они это делают в отношении этого Парламента и Департамента парламентских услуг, и с точки зрения технических рекомендаций, которые они получают, они взять это из Центра кибербезопасности Австралийского управления сигналов».

Бёрджесс сказал, что ASIO обратится в департамент, если у него возникнут проблемы с безопасностью в связи со шпионажем, иностранным вмешательством, саботажем или какие-либо проблемы безопасности, которые его волнуют.

«Мы бы участвовали, если бы происходили действия, которые заставляли нас выбирать расследование, чтобы убедиться, что имел место или имел место человек, какой-либо шпионаж или кибершпионаж - мы расследуем такие вопросы, и мы делаем это совместно с люди, которые нам были нужны», - добавил он.

Парламентская сеть и политические партии Австралии не смогли успешно защитить себя во время атаки в феврале 2019 года.

В течение восьми дней злоумышленник, описанный как государственный деятель, мог оставаться в сети, поражая всех, у кого есть адрес электронной почты здания парламента Австралии, включая политиков и всех их сотрудников». ***(Asha Barbaschow. ASIO boss says he's not concerned with Australian Parliament's March outage // ZDNet (https://www.zdnet.com/article/asio-boss-says-hes-not-concerned-with-australian-parliaments-march-outage/). 14.04.2021).***

***

«Служба электронной почты Google - Gmail - «более безопасна», чем система электронной почты парламента, заявил председатель Специального комитета по иностранным делам.

Том Тугендхат сказал в программе Today на BBC Radio 4, что за последние три года он неоднократно становился объектом кибератак.

Он сказал BBC, что хакеры пытались получить доступ к его аккаунту и отправляли электронные письма, выдавая его за него.

Депутат-консерватор считает, что за некоторыми из этих попыток стояли Китай и Иран.

«Друзья из GCHQ сказали мне, что мне лучше придерживаться Gmail, чем использовать парламентскую систему, потому что она более безопасна», - сказал г-н Тугендхат.

«Откровенно говоря, это говорит вам об уровне безопасности и приоритете, который мы придаем демократии в Соединенном Королевстве».

Пресс-секретарь сообщила, что система парламентской электронной почты «предлагает значительно более высокий уровень безопасности, чем внешние провайдеры».

Национальный центр кибербезопасности заявил, что депутаты должны продолжать использовать парламентскую систему электронной почты.

Г-н Тугендхат является одним из многих британских политиков, на которых Китай наложил санкции за то, что он считает распространением «лжи и дезинформации» о нарушениях прав человека уйгурского населения в районе Синьцзян в Китае.

Санкции запрещают г-ну Тугендхату, который возглавляет China Research Group вместе с другим консерватором Нилом О'Брайеном, ездить в Китай.

«На прошлой неделе были разосланы электронные письма, в которых утверждалось, что я исходил от меня, и утверждалось, что я ушел из комитета по иностранным делам».

Он добавил, что «многие другие кибератаки были совершены либо на меня, либо на других», и намекнул, что атаки были связаны с недавними санкциями Китая.

Тара Уиллер, научный сотрудник Школы государственного управления Кеннеди Гарвардского университета, охарактеризовала Gmail как «очень безопасный выбор электронной почты», но сказала, что для обеспечения безопасности необходимо наличие программы расширенной защиты с ключом безопасности и многофакторной аутентификацией. высочайший уровень безопасности.

«Это то, что я и многие другие специалисты по безопасности использую для нашей электронной почты и рекомендую членам семьи».

Правительство часто уделяет первоочередное внимание удобству использования, и «иногда безопасность становится дорого обходиться», - добавила она.

«ИТ-администраторы, которые работают над тем, чтобы сбалансировать все эти вещи, часто недофинансируются - и их поддержка невероятно важна для повышения безопасности государственных систем».

Но доктор Стефани Хэйр, исследователь технологий, сказала, что парламент должен иметь «гораздо большую безопасность, чем Gmail».

«Я не удивлен, узнав, что адреса электронной почты депутатов становятся мишенями - этого и следовало ожидать.

«Все системы уязвимы, но мы хотели бы видеть максимально возможную безопасность систем электронной почты, используемых нашими избранными должностными лицами, чтобы защитить нашу демократию», - сказала она». ***(Cristina Criddle. Gmail 'safer than parliament's email system' says Tory MP // BBC (https://www.bbc.com/news/technology-56733667). 13.04.2021).***

***

«Концепция холодной войны не устарела. За десятилетия, прошедшие после распада Советского Союза, поле боя просто переместилось от конфликтов между идеологическими прокси-правительствами к киберпространству. А противники выросли из нескольких основных стран в широкий круг субъектов суверенной угрозы.

Вопрос в том, когда кибератака пересекает грань между преступным действием или простым розыгрышем и актом войны? Это природа жертвы? Характер злоумышленника? Характер повреждений? Или их все вместе?

Безусловно, это решение не для профессионалов в области кибербезопасности. Наша роль заключается в защите ИТ-активов наших организаций путем снижения рисков, устранения угроз, исправления ситуации после атаки и в целом попыток обеспечить безопасную и бесперебойную работу всего. Неважно, сталкиваемся ли мы с сценаристом, пытающимся испортить веб-сайт, политическим хактивистом, пытающимся сделать заявление, киберпреступником, пытающимся украсть или выкупить наши данные, или государственным деятелем, пытающимся украсть конфиденциальную информацию. Наша цель - не допустить их и свести к минимуму ущерб, когда им удастся проникнуть внутрь. Единственное, что изменится, - это то, насколько хорошо обеспечены ресурсами и упорны наши противники.

Определение акта войны

Оксфордский справочный словарь определяет акт войны как: «Действие одной нации, направленное на развязывание или спровоцирование войны с другой страной; акт считается достаточным поводом для войны». Это хорошее определение, но оно оставляет некоторую двусмысленность в применении к сфере кибербезопасности. Он фокусируется на намерении, причем первостепенное значение имеет причина действия; и он определяет преступника и цель как суверенные государства.

Оксфордское определение вызывает несколько вопросов. Как вы относитесь к актам шпионажа (политического, промышленного или иного) в этом контексте? Считается ли деструктивным заражение промышленного оборудования страны специально разработанным вирусом, вызвавшим его отказ? Как насчет заражения государственного поставщика и последующего использования этой уязвимости для вторжения в государственные ведомства вашего конкурента? Оба случая имеют огромное влияние на конкурирующее государство, хотя цель не состояла в том, чтобы спровоцировать перестрелку.

А как насчет случаев, когда антагонист - не спонсируемая государством организация, а скорее преступная или активистская организация, пользующаяся государственной поддержкой? Защищает ли правдоподобное отрицание правительство от последствий этих действий? Конечно, возможно и обратное: независимая преступная организация или активистская организация, совершающая инцидент, который воспринимается как спонсируемый государством.

Исторические примеры, такие как взлом SolarWinds, обнаруженный в декабре, или червь Stuxnet десятилетней давности, были крупными инцидентами с серьезными политическими и дипломатическими последствиями. Но ни то, ни другое не привело к войне. И это хорошо. Пока что инциденты в киберпространстве не переросли в перестрелку в реальном мире. Но так бывает не всегда.

Что пересекает черту?

Учитывая, что большая часть мировой инфраструктурной сети включена и уязвима для атак, логично предположить, что какой-то субъект где-то где-то может

пересечь черту. Противник может разрушить жизненно важную инфраструктуру или вызвать инцидент, который непосредственно приведет к гибели многих людей. Электросеть. Управления воздушным движением. Множество других систем, потенциально уязвимых для атак, могут стать спусковым крючком, подталкивающим суверенное государство к войне.

Возможно, тогда повезло, что гражданским организациям не разрешено ни по закону, ни с этической точки зрения «открывать ответный огонь» в случае кибератаки. В свою очередь, военные и разведывательные организации продемонстрировали здравый смысл, чтобы держать свои реакции тайными или скрытыми в тех случаях, когда они принимали непосредственное участие.

Нет никаких сомнений в том, что в киберпространстве идет своего рода холодная война. Возможно, игроки изменились. Может возникнуть некоторая двусмысленность в том, кто на кого работает. И цели расширились. Но это происходит. К счастью, ей еще предстоит перейти черту и проявиться в реальном мире как горячая война.

Как профессионалы в области кибербезопасности, наша часть остается прежней; чтобы обезопасить наши организации от кибератак. Если мы обучим наших пользователей и будем обновлять наши процессы и инструменты, не будет иметь значения, атакованы ли мы скрипачом или иностранной державой. Наша оборона устоит, а если нет, мы сможем навести порядок.

Выяснение того, был ли это акт войны, выпадет на долю политиков и дипломатов - где ему и место». ***(Saryu Nayyar. Crossing the Line: When Cyberattacks Become Acts of War // Threatpost (https://threatpost.com/crossing-line-cyberattack-act-war/165290/). 07.04.2021).***

***

«Исследователи сообщили, что во Вьетнаме была обнаружена продвинутая кампания кибершпионажа, направленная на правительственные и военные структуры, в рамках которой был предоставлен инструмент удаленного доступа (RAT) для проведения шпионских операций.

Дальнейший анализ показал, что эта кампания проводилась группой, связанной с китайскоязычной продвинутой постоянной угрозой (APT), известной как Cycldek (также известной как Goblin Panda, APT 27 и Conimes), по словам исследователей Kaspersky, которые добавили, что группа была активна как минимум с 2013 года.

Вредоносная программа, используемая в кампании, получившая название FoundCore, позволяет злоумышленникам манипулировать файловой системой, процессами, делать снимки экрана и выполнять произвольные команды.

Согласно анализу, опубликованному «Лабораторией Касперского» в понедельник, это представляет собой серьезный прорыв в развитии группы. Например, по словам исследователей, метод, используемый для защиты вредоносного кода от анализа, является уникальным для китайскоязычных групп.

«Заголовки (место назначения и источник кода) для окончательной полезной нагрузки были полностью удалены, а те немногие, которые остались, содержали несогласованные значения», - пояснили они. «Поступая так, злоумышленники

значительно усложняют исследователям обратное проектирование вредоносного ПО для анализа. Более того, компоненты цепочки заражения тесно связаны, а это означает, что отдельные части сложно, а иногда и невозможно анализировать изолированно, что не позволяет получить полную картину вредоносной активности».

В кампании также используется загрузка неопубликованных библиотек с динамической компоновкой (DLL), которая происходит, когда законно подписанный файл обманом загружает вредоносную DLL, позволяя злоумышленникам обойти продукты безопасности.

«В этой недавно обнаруженной кампании цепочка заражения боковой загрузкой DLL выполняет шелл-код, который расшифровывает окончательную полезную нагрузку: [FoundCore], что дает злоумышленникам полный контроль над зараженным устройством», - говорится в анализе.

FoundCore: 4 потока вредоносных программ

Последняя полезная нагрузка в цепочке заражения - это инструмент удаленного администрирования, который обеспечивает полный контроль над машиной жертвы для ее операторов. По словам исследователей, после выполнения эта вредоносная программа запускает четыре потока:

Первый устанавливает настойчивость путем создания службы.

Второй устанавливает незаметную информацию для службы, изменяя ее поля Description, ImagePath и DisplayName (среди прочего).

Третий устанавливает пустой дискреционный список управления доступом (DACL) к изображению, связанному с текущим процессом, чтобы предотвратить доступ к базовому вредоносному файлу. DACL - это внутренний список, прикрепленный к объекту в Active Directory, который указывает, какие пользователи и группы могут получить доступ к объекту и какие операции они могут выполнять с объектом.

Наконец, рабочий поток запускает выполнение и устанавливает соединение с сервером C2. В зависимости от конфигурации он также может внедрить свою копию в другой процесс.

Связь с сервером может происходить либо через необработанные сокеты TCP, зашифрованные с помощью RC4, либо через HTTPS.

В цепочке заражения обнаружено, что FoundCore загружает еще две части шпионского ПО. Первый, DropPhone, собирает информацию об окружающей среде с машины жертвы и отправляет ее в DropBox. Второй, CoreLoader, запускает код, который помогает вредоносному ПО ускользать от обнаружения продуктами безопасности.

«В целом, за последний год мы заметили, что многие из этих китайскоязычных групп вкладывают больше ресурсов в свои кампании и оттачивают свои технические возможности», - сказал Марк Лехтик, старший исследователь безопасности в Kaspersky, в анализе. «Здесь они добавили гораздо больше уровней обфускации и значительно усложнили обратный инжиниринг. И это сигнализирует о том, что эти группы могут стремиться к расширению своей деятельности».

Вьетнам в APT Sights

Анализ «Лаборатории Касперского» показал, что в кампании были задействованы десятки компьютеров, подавляющее большинство (80%) которых расположено во Вьетнаме. Остальные цели были обнаружены в Средней Азии и Таиланде.

Фирма также обнаружила, что большинство жертв принадлежали правительству или военному сектору. При этом были и другие целевые сектора, включая дипломатию, образование и здравоохранение.

«Прямо сейчас может показаться, что эта кампания представляет собой скорее локальную угрозу, но весьма вероятно, что бэкдор FoundCore в будущем будет обнаружен в большем количестве стран в разных регионах», - сказал Лехтик.

Пьер Делшер, старший исследователь безопасности в Kaspersky, добавил: «Более того, учитывая, что эти китайскоязычные группы склонны делиться своей тактикой друг с другом, мы не удивимся, обнаружив такую же тактику обфускации в других кампаниях. Мы будем внимательно следить за ландшафтом угроз на предмет аналогичной подозрительной активности. Для компаний лучшее, что они могут сделать, - это держать свою компанию в курсе последних аналитических данных об угрозах, чтобы они знали, на что обращать внимание». ***(Tara Seals. Spy Operations Target Vietnam with Sophisticated RAT // Threatpost (https://threatpost.com/spy-operations-vietnam-rat/165243/). 05.04.2021).***

***

«Российские хакеры по-прежнему проводят наступательные кибератаки против США и их союзников, пытаясь украсть информацию или заложить основу для будущих операций, говорится в совместном предупреждении служб безопасности и разведки.

В сообщении ФБР, Департамента внутренней безопасности и CISA содержится предупреждение о том, что Служба внешней разведки России (СВР), также известная исследователям кибербезопасности как APT 29, Dukes и CozyBear, продолжает атаковать организации, пытаясь собрать разведывательную информацию.

Агентства США вместе с Национальным центром кибербезопасности Великобритании (NCSC) недавно обвинили SVR в атаке на цепочку поставок SolarWinds, в результате которой хакеры взломали процесс обновления программного обеспечения компании и получили доступ к системам в девяти государственных учреждениях и около 100 компаниях частного сектора.

А теперь организации предупреждают, что российские кибератаки не показывают признаков замедления, особенно когда речь идет о нацеленных на сети организаций, связанных с правительством, аналитическими центрами и информационными технологиями.

Облачные сервисы, включая электронную почту и Microsoft Office 365, подвергаются атакам.

«Нацеливание на облачные ресурсы, вероятно, снижает вероятность обнаружения за счет использования скомпрометированных учетных записей или неправильной конфигурации системы для смешивания с обычным или

неконтролируемым трафиком в среде, недостаточно защищенной, контролируемой или понятной для организаций-жертв», - предупреждает агентство.

В предупреждении подробно описаны распространенные методы, используемые в операциях SVR, включая распыление паролей, использование уязвимостей нулевого дня и развертывание вредоносных программ.

Распыление паролей - это когда злоумышленники нацелены на слабые пароли, связанные с учетными записями администратора. Эти учетные записи защищены обычными или ненадежными паролями, включая имена пользователей и пароли по умолчанию, что дает кибератакам относительно простые средства получения доступа к плохо защищенным сетям.

Во многих случаях злоумышленники взламывают как можно больше учетных записей, думая только о том, как их можно использовать позже.

Чтобы защититься от атак с использованием паролей, ФБР и DHS рекомендуют обязательное использование многофакторной аутентификации в сети и, по возможности, принудительное использование надежных паролей - особенно для учетных записей администраторов. Также рекомендуется запретить доступ к удаленным административным функциям с IP-адресов, не принадлежащих организациям.

Другой распространенный метод атаки, используемый хакерами, поддерживаемыми Кремлем, - это использование уязвимостей в устройствах виртуальной частной сети (VPN), которые раскрывают учетные данные для входа.

В предупреждении используется пример использования злоумышленниками CVE-2019-19781 - уязвимости в контроллере доставки приложений Citrix и шлюзе - но это одна из нескольких, которые использовались в кибератаках в последние годы, позволяя злоумышленникам тайно проникать в сети.

В каждом из этих случаев затронутый поставщик выпустил критическое исправление безопасности - а в некоторых случаях они были доступны в течение многих лет, - но организации, которые не применяют обновления, по-прежнему уязвимы для атак.

ФБР, Министерство здравоохранения и CISA также предупреждают об атаках с использованием WellMess - формы настраиваемого вредоносного ПО, связанного с APT 29, которое использовалось в атаках, нацеленных на объекты по исследованию вакцины COVID-19. Хотя украденные учетные данные RDP использовались для установки вредоносного ПО, также известно, что злоумышленники пытались распространить его через целевые фишинговые электронные письма.

Предупреждение о российских методах взлома было выпущено, чтобы побудить организации изучить свои сети и лучше понять, как защитить их от атак.

«ФБР и DHS предоставляют информацию о кибер-инструментах, целях, методах и возможностях SVR, чтобы помочь организациям в проведении собственных расследований и обеспечении безопасности своих сетей», - говорится в предупреждении». ***(Danny Palmer. FBI: Russian hackers are still trying to break into networks, here's how to protect yours from attack // ZDNet (https://www.zdnet.com/article/fbi-russian-hackers-are-still-trying-to-break-into-networks-heres-how-to-protect-yours-from-attack/). 27.04.2021).***

***

Кібератака на SolarWinds

«Соединенное Королевство, Канада, Европейский Союз и НАТО выразили поддержку Соединенным Штатам, обвиняющим Россию в кибератаке на управляющую ИТ-компанию SolarWinds, которая затронула организации по всему миру.

Объявления были сделаны в тот же день, когда Соединенные Штаты выслали 10 российских дипломатов и наложили санкции на десятки компаний и людей в попытке наказать Россию, которая, как считается, в прошлом году организовала как вмешательство в президентские выборы в США, так и нарушение политики SolarWinds.

Администрация Байдена заявила, что санкции должны были послать Кремлю сигнал о том, что США готовы принять меры против усилий, которые подрывают «проведение свободных и справедливых демократических выборов и демократических институтов в Соединенных Штатах, их союзниках и партнерах», или те, которые «способствуют злонамеренным действиям в киберпространстве против США, их союзников и партнеров».

Канада в четверг заявила, что взлом SolarWinds затронул более сотни канадских организаций, но ей неизвестно о том, чтобы кто-либо из них был скомпрометирован в ходе последовавшей за этим кампании кибершпионажа.

«Канада считает, что APT29, также именуемый «Герцоги» или «Уютный медведь», был ответственен за эту деятельность и почти наверняка действует как часть российских разведывательных служб (СВР). Эта деятельность вызывает обеспокоенность, учитывая историю подрывной и дестабилизирующей кибернетической деятельности других российских субъектов, спонсируемых государством. Мы выражаем нашу озабоченность, чтобы подчеркнуть важность укрепления кибербезопасности нашей страны», - заявила Канада.

Европейский союз отметил, что Solarwinds кибер-операции оказали влияние на правительства и бизнеса в странах - членах ЕС также выражают озабоченность по поводу возросшей активности таргетирования «безопасность и целостность информационных и коммуникационных технологий (ИКТ) продукции и услуг.»

В четверг НАТО сообщило, что его союзники принимают меры по укреплению коллективной безопасности, добавив, что Россия продолжает дестабилизирующее поведение путем попыток вмешательства в выборы, широкомасштабных кампаний дезинформации и злонамеренных кибератак.

«Соединенные Штаты и другие союзники считают, что все имеющиеся свидетельства указывают на ответственность Российской Федерации за взлом SolarWinds. Мы солидарны с Соединенными Штатами», - заявили в НАТО, призвав Россию прекратить такое поведение.

Как и США, Великобритания в четверг напрямую обвинила Кремль в атаке на SolarWinds, назвав Россию «самой серьезной угрозой национальной и

коллективной безопасности Великобритании». Великобритания также опубликовала дополнительную информацию о кибер-деятельности SVR.

В сообщении в четверг Агентство национальной безопасности (АНБ) предупредило о российских хакерских операциях, направленных на пять известных и уже исправленных уязвимостей, включая уязвимости, затрагивающие Fortinet FortiGate VPN, Synacor Zimbra Collaboration Suite, Pulse Secure Pulse Connect Secure VPN, Citrix Application Delivery Controller и Шлюз и VMware Workspace ONE Access». ***(Ionut Arghire. More Countries Officially Blame Russia for SolarWinds Attack // Wired Business Media (https://www.securityweek.com/more-countries-officially-blame-russia-solarwinds-attack). 16.04.2021).***

***

Захист персональних даних

«В то время как правительство Германии все еще борется с проектом Закона об ИТ-безопасности 2.0 и адаптацией правил, касающихся штрафов, органы по защите данных государств-членов ЕС уже установили факты на основе Общего регламента ЕС по защите данных («GDPR»). Многие штрафы, наложенные с мая 2018 года, были вызваны недостаточными мерами кибербезопасности. Что произошло?

В соответствии со статьей 32 (1) GDPR контролер обязан принять достаточные технические и организационные меры для обеспечения безопасности обработки данных, осуществляемой через ИТ-системы. Меры, необходимые в конкретном случае, определяются, среди прочего, уровнем техники, затратами на реализацию, типом, объемом, обстоятельствами и целями обработки данных, а также различной вероятностью и серьезностью риска для прав и свободы субъектов данных.

Но что компании могут извлечь из различных судебных разбирательств?

1. Марриотт

Орган по защите данных Великобритании, ICO, вызвал ажиотаж в 2018 году, когда наложил на миллиардную компанию Marriott International Inc. (Marriott) штраф в размере миллионов евро.

Предпосылкой к этому послужило то, что Marriott приобрела гостиничную сеть Starwood в 2016 году, не пересмотрев меры кибербезопасности компании. Уже в 2014 году системы Starwood были атакованы хакерами с целью извлечения информации о клиентах. На момент приобретения этого замечено не было. Только в 2018 году утечка данных была обнаружена и сообщена ICO. К тому времени уже было получено доступ к 339 миллионам клиентских записей. Первоначально установив штраф в размере 99,2 миллиона фунтов стерлингов (~ 115 миллионов евро), ICO снизило его до 18,4 миллиона фунтов стерлингов (~ 20,4 миллиона евро) благодаря хорошему сотрудничеству с Marriott.

Кейс показывает, что особое внимание необходимо уделять структуре кибербезопасности приобретаемой компании. Если компания не приняла

достаточных технических и организационных мер для защиты данных, это необходимо определить и немедленно исправить. В противном случае покупателю угрожают киберриски, которые могут привести к значительному косвенному ущербу для компании. Здесь следует думать не только о потенциальной угрозе штрафов, но и о претензиях о возмещении ущерба пострадавшими, а также о возмещении ущерба, который может возникнуть в результате использования информации (например, коммерческой тайны). Хакеры могут использовать ситуацию для попыток шантажа.

2. Доступ к данным о здоровье

Неоднократно выявлялись случаи, когда не принимались достаточные меры для ограничения доступа к данным о состоянии здоровья. Данные о здоровье - это особая категория персональных данных (статья 9 (1) GDPR), которая подлежит особенно высокому уровню защиты.

С момента вступления в силу GDPR органы по защите данных неоднократно применяли санкции. Первый штраф такого рода был наложен на государственную больницу в Португалии, поскольку медицинский персонал имел неограниченный доступ к данным о здоровье пациентов - в некоторых случаях даже через фальсифицированные профили. Штраф составил 400 000 евро. С тех пор такие случаи неоднократно выявлялись - например, в Нидерландах или Норвегии. В частности, в Швеции в связи с этим было наложено пять различных штрафов. Самая высокая из них была направлена против больницы Capio St. Göran и составила 30 миллионов шведских крон (2,9 миллиона евро).

Каталог обязательств по статье 32 GDPR также включает защиту данных от несанкционированного внутреннего доступа. Это особенно верно, когда речь идет о «конфиденциальных» данных, таких как данные о состоянии здоровья. Опасность доступа к данным возникает не только извне в результате хакерских атак, но и представляет реальный риск внутри самой компании. Этому нужно противодействовать. Защитные меры также должны быть адаптированы к потенциальному риску, который особенно неизбежен в случае несанкционированной обработки «конфиденциальных» данных.

3. 1 & 1 Telecom GmbH

Дело 1 & 1 Telecom GmbH («1 & 1»), вероятно, станет особенно печально известным. Не только потому, что Федеральный комиссар по защите данных и свободе информации («BfDI») первоначально наложил штраф в размере 9,55 миллиона евро, но и потому, что это первое дело о наложении штрафа GDPR, вынесенном обычным судом в Германии. BfDI наложил штраф в размере 9,55 млн евро на 1 & 1 в 2019 году. Предпосылкой для этого было то, что, по мнению BfDI, требований аутентификации в колл-центре 1 & 1 было недостаточно. В то время 1 & 1 запрашивали только имя и дату рождения для аутентификации, а это означало, что бывший партнер клиента, знающий эти данные, мог найти номер телефона и дату разблокировки в 1 & 1. Боннский окружной суд счел наложение штрафа оправданным, но сумма казалась необоснованной. Штраф был уменьшен до 900 000 евро.

Однако случай 1 & 1 - не первый случай, когда речь идет о неадекватных мерах аутентификации. В Нидерландах был аналогичный случай, когда

Arbeitnehmerversicherungsagentur (UWV) (Агентство по страхованию сотрудников) также было оштрафовано на 900 000 евро из-за неадекватности процесса аутентификации для онлайн-портала. Это позволило перекачивать данные рабочих. Во Франции было также дело SERGIC. Здесь можно получить доступ к конфиденциальным данным потенциальных арендаторов без предварительной аутентификации. Французский орган по защите данных CNIL наложил штраф в размере 400 000 евро.

Поэтому компаниям предлагается не только выбрать процедуру аутентификации, которая предотвращает вероятность неправомерного использования, но также разрабатывать и постоянно улучшать ее в соответствии с современным уровнем техники. Это также относится ко всем другим техническим и организационным мерам…». ***(Mareike Christine Gehrmann. Gaps in cyber security protection? A risk of fines! // Taylor Wessing (https://iot.taylorwessing.com/gaps-in-cyber-security-protection-a-risk-of-fines/). 16.04.2021).***

***

«Недавний опрос израильской компании CyberArk, лидера в области защиты личных данных, показал, что около 97% руководителей высшего звена службы безопасности считают, что злоумышленники все чаще стремятся украсть их корпоративные учетные данные. По мере того, как организации переносят свои активы в защищенные облачные сети и расширяют доступ третьих сторон к своим ресурсам, позволяя модели удаленной работы, в корпоративных сетях обнаруживаются слабые места, которые могут быть не полностью защищены.

Отчет CyberArk под названием «Обзор CISO View 2021: нулевое доверие и привилегированный доступ» показал, что среди руководителей высшего звена и представителей отрасли кибербезопасности растет беспокойство по поводу того, что киберпространство становится менее безопасным, и существует срочная необходимость обеспечения безопасности и защиты доступа. в корпоративные сети. CyberArk в основном занимается ограничением управления доступом и предоставляет комплексные предложения по безопасности для распределенных рабочих групп и рабочих нагрузок гибридного облака, помогая защитить и обеспечить безопасность наиболее важных активов корпораций.

Опрос показал, что группа наибольшего риска, сталкивающаяся с наибольшим числом увеличивающихся атак, - это конечные пользователи или бизнес-пользователи, имеющие доступ к конфиденциальным данным. Около 56% респондентов считают, что такие люди стали жертвами кибератак. Это верно для руководителей высшего звена (48%), сторонних поставщиков и подрядчиков (39%), DevOps и облачных инженеров (33%). Также участились попытки кражи учетных данных для личных данных (70%), а также для финансовых систем и данных (66%). Это подчеркивает заинтересованность злоумышленников в получении доступа к высокочувствительным системам, которые часто принадлежат конечным пользователям, а не администраторам.

В ответ на эти тревожные цифры данных руководители службы безопасности заинтересованы во внедрении подхода нулевого доверия, в котором

кибербезопасность усиливается, признавая, что доверие - это уязвимость, которую необходимо ограничивать. Около 88% опрошенных респондентов считают, что принятие такого подхода «очень важно» или «важно». Для реализации такой модели главным приоритетом будет сосредоточение внимания на управлении идентификацией и доступом, которое было выбрано 45% респондентов как «важное». Респонденты отдали предпочтение и другим типам контроля, а контроль доступа «точно в срок» выбрали 87% респондентов, которые считали, что ограниченные постоянные привилегии являются «важным» или «очень важным» аспектом Zero Trust.

Поскольку хакеры могут использовать слабые места, растет потребность в решениях безопасности, которые работают, несмотря на внутренние ограничения. Около 94% респондентов заявили, что безопасность конечных точек «важна», а 46% заявили, что установка такого программного обеспечения в сетях является сложной задачей. Кроме того, 86% были обеспокоены тем, что может навредить оптимизации взаимодействия с пользователем, заявив, что это «важно» или «очень важно», но подчеркнули необходимость того, чтобы инструменты и политики безопасности не игнорировались или просто игнорировались из-за неаккуратного поведения.

«Отголоски атаки SolarWinds по-прежнему подчеркивают необходимость защиты привилегированных учетных данных и разрыва цепочки атак на наиболее ценные активы организации», - сказал Майк О'Мэлли, старший вице-президент CyberArk по глобальному маркетингу. «По мере того, как на предприятии растет число новых идентификационных данных, в этом обзоре подчеркивается важность подхода на основе нулевого доверия к Identity Security. Мы считаем, что для руководителей службы безопасности, стремящихся снизить риски целевого фишинга, атак с подделкой от других лиц и других форм компрометации, опыт взаимодействия, отраженный в отчетах CISO View, станет бесценным инструментом, независимо от того, где их организация находится на стадии зрелости с нулевым доверием. -изгиб."

Опрос был частью пятого в серии обзоров CISO View и основывался на подробных интервью с 12 высшими руководителями служб безопасности из компаний Global 1000, проведенных в четвертом квартале 2020 года. Серия CISO View была создана при содействии независимого агентства. исследовательская фирма Robinson Insight». ***(Survey: Cybersecurity executives see increase in attempted credential theft // CTech (https://www.calcalistech.com/ctech/articles/0,7340,L-3904075,00.html). 11.04.2021).***

***

«Чем больше становится Интернет-супермагистраль информации; тем больше пользователей сталкивается с нарушениями конфиденциальности и кражей данных. Если бы только мы могли перестроить инфраструктуру Интернета, чтобы сделать передачу данных более безопасной и надежной, - это общий призыв экспертов в области ИТ и кибербезопасности.

В настоящее время предпринимаются некоторые усилия по уменьшению проблем с конфиденциальностью и кражей данных. Но, несмотря на то, что время

от времени появлялись предложения заменить Интернет на новую улучшенную супермагистраль, текущие проекты сродни заделке выбоин и ремонту полос движения на физических транзитных дорогах.

Недавнее исследование Digital Lab Consumer Reports показывает, что 96 процентов американцев согласны с тем, что необходимо делать больше для защиты конфиденциальности потребителей. Но не ожидайте появления в ближайшее время совершенно нового альтернативного Интернета.

Вместо этого вы увидите, что основное внимание уделяется программным предложениям, основанным на конфиденциальности и безопасности, а не на оборудовании. Эти «заплатки» включают новый альтернативный поиск, браузеры, электронную почту, чат, производительность, платежи и решения AdTech.

Одна из компаний, взявших на себя инициативу по исправлению положения в Интернете, - это The @ Company. Его генеральный директор Барбара Таллент хочет обеспечить более безопасный и ориентированный на человека Интернет, основанный на предоставлении вам подлинного владения и контроля над вашими личными данными.

С этой целью компания в октябре прошлого года запустила приложение, основанное на своем новом протоколе конфиденциальности. Этот новый стандарт попытается изменить то, как онлайн-продавцы и компании работают с личной информацией миллиардов пользователей Интернета.

Цель состоит в том, чтобы взять под контроль вашу пользовательскую информацию от других и вернуть ее вам. Согласно Талленту, каждый бит личной информации в Интернете собирается, хранится, систематизируется и используется для продажи, отслеживания и даже профилирования всех на планете, включая вас.

"Определенно существует тенденция к конфиденциальности, но я бы сказал, что более конкретно люди хотят иметь возможность доверять тому, что данные, которые они предоставляют, используются для намеченных целей, не отслеживаются, и что, как только они предоставили данные, они право быть забытым и участвовать анонимно», - сказала она TechNewsWorld.

Исправляем то, что сломано

Обсуждая проблемы, связанные с воздействием на Интернет, Таллент отметил, что уже доступен ряд обходных решений. Она ожидает, что скоро будет еще больше.

Например, теперь вы можете получить телефоны без Google. В e.foundation предлагает первый из таких телефонов в 2021 году Более де-Гугле телефонов ожидается в этом году будет выпущен из Osom продуктов. Эти телефоны не будут использовать ваши данные в собственных целях.

Еще одно исправление для приложений для обмена сообщениями. В 2020 году Signal и Telegram лидировали в сфере обмена личными сообщениями, предложив сквозное шифрование. В 2021 году следующее поколение приложений для обмена сообщениями позволит вам удалять свои сообщения с чужого телефона, если вы того пожелаете. Скоро ваши сообщения всегда будут принадлежать только вам.

В этом году также появятся улучшения в области обмена файлами; 2021 год принесет настоящий одноранговый обмен файлами. Полностью зашифрованные файлы можно передавать без постоянного хранения на сервере в облаке.

Также обратите внимание на совместное использование местоположения. В этом году вы сможете делиться своим местоположением в частном порядке с семьей и друзьями и разрешить обмен данными о местоположении с другими организациями, если их об этом попросят.

Также мы увидим контроль контактных данных. Контактные приложения позволят вам контролировать доступ к своей информации в 2021 году, - предлагает Таллент.

Социальные медиа

В 2020 году мы начали наблюдать рост частных социальных сетей, построенных на таких сайтах, как Mastodon. Затем, когда консерваторы стали подвергаться все большей цензуре на YouTube и Facebook, они обратились к таким сайтам, как Parler.

Эта тенденция сохранится и в 2021 году, поскольку сайты социальных сетей позволяют более детально классифицировать людей, а не просто «подписчиков» и «друзей». Эти «группы» можно использовать в нескольких приложениях, что делает их более интересными, полезными и увлекательными.

«В настоящее время ваши данные распространяются по всему Интернету. К счастью, создаются новые компании, которые помогают вам вернуть эти данные», - продолжила она.

Например, в прошлом году Mine объявила, что может выяснить, у каких компаний есть ваши данные, насколько они потенциально уязвимы и как удалить их с серверов этих компаний. По мере расширения этих услуг в 2021 году многие компании столкнутся с обесцениванием своих хранилищ массовых данных и могут быть вынуждены обратиться к другим бизнес-моделям.

«Когда у вас будет настоящая конфиденциальность и возможность получать информацию, в этом пространстве появятся новые интересные приложения. Примером может служить приложение для голосования, которое позволяет вам проводить опросы среди ваших друзей конфиденциально и анонимно», - сказала она.

Существуют обходные пути

«Существует три основных типа решений, которые используются на протяжении десятилетий для защиты данных, пересылаемых через Интернет», - отметил Таллент.

Во-первых, шифрование данных на лету с помощью прозрачного уровня безопасности (TLS) или виртуальных частных сетей (VPN). Во-вторых, зашифруйте данные в стенах приложения. В-третьих, создайте модели управления доступом на уровне приложений и соответствующие им процессы.

«Совсем недавно открытые протоколы, такие как протокол Signal, позволили в различных вариантах использования, таких как обмен мгновенными сообщениями, использовать ту же криптографию и программное обеспечение для обеспечения сквозного шифрования», - отметил Таллент.

«Signal, Skype и WhatsApp используют протокол Signal. Но, к сожалению, вы не можете отправить мгновенное сообщение из Signal в Skype или WhatsApp. Кроме того, сквозного шифрования недостаточно», - сказала она.

Конфиденциальность на скользком спуске

Независимо от того, используется ли для частного или коммерческого использования, то, как конфиденциальность обеспечивается обменом сообщениями и другими приложениями, может быть движущейся целью. Например, рассмотрим публичный всплеск и миграцию пользователей из WhatsApp в приложение для чата Signal, ориентированное на конфиденциальность, в начале этого года.

WhatsApp утверждает, что он зашифрован, и основная часть активности в приложении - это. Но того факта, что Facebook может узнать, когда вы использовали приложение и с кем вы общались, для миллионов людей было достаточно, чтобы потерять доверие клиентов, считает Таллент.

«Возвращение ключей владельцам данных и разделение связи между данными и уровнями приложений меняют правила игры. Но предоставление платформы и SDK для разработчиков внешнего интерфейса для разработки новых возможностей без необходимости сосредоточиваться на инфраструктуре и сложностях криптографических обменов. это то, что волнует всех нас в сообществе [безопасности]», - отметила она.

Мнения разнятся

Нет необходимости в замене Интернета. Технологическим отраслям нужно только расставить приоритеты в своих ресурсах для разработки более эффективных способов усиления своей политики кибербезопасности, снижения риска атак, заметил Стивен Лайт, владелец Nolah, продавца матрасов и постельных принадлежностей в электронной торговле.

«Текущая безопасность Интернета достаточна, чтобы ограничить пользователей, которые не знают, как обойти кибербезопасность. Однако ситуация иная для опытных хакеров, [которые] могут проникнуть в систему, если они проявляют терпение и осторожны, чтобы не быть обнаруженными. ", - сказал он TechNewsWord.

Исправление Интернета - амбициозная цель. Это также немного похоже на замену шин во время движения автомобиля, - предположил Пурандар Дас, генеральный директор и соучредитель Sotero, компании по обеспечению безопасности на основе шифрования.

«Более важно, чтобы организации приняли более значимую стратегию безопасности и конфиденциальности применительно к потребителям. Создание равных условий для безопасности и конфиденциальности наравне с техническими возможностями и потоками доходов имеет решающее значение», - сказал он TechNewsWorld.

Что-то должно измениться в том, как мы обеспечиваем безопасность в Интернете. Многие люди понятия не имеют, насколько уязвима их личная и конфиденциальная информация для хакеров и других киберпреступников, соглашается Дайват Дхолакия, операционный директор Force by Mojio, службы GPS-слежения за парком транспортных средств для малого бизнеса.

«В то время как такие компании, как Facebook, склонны подчеркивать важность индивидуального контроля над настройками безопасности, реальная ответственность лежит на гигантских технологических компаниях, которые ежедневно обрабатывают нашу информацию. Они должны быть более прозрачными в отношении того, кому они предоставляют и продают вашу информацию, и им необходимо усилить свои подразделения по кибербезопасности», - сказал он TechNewsWorld.

Дхолакия считает, что серьезное обновление интернет-безопасности неизбежно. Но это будет многолетний проект, осложненный тем фактом, что компании, покупающие и использующие данные, заинтересованы в том, чтобы настройки конфиденциальности оставались отключенными или недоступными.

«В конце концов, я не думаю, что Интернет куда-то денется, но я думаю, что через 10 лет мы будем использовать совершенно другой вид Интернета», - предсказал он.

Что необходимо и жизнеспособно

Вместо того, чтобы создавать совершенно новый Интернет с нуля, компании, ориентированные на конфиденциальность, применяют проверенные и хорошо изученные технологические альтернативы, которые разделяют тезис об отсутствии слежки и предоставлении людям контроля над своими данными.

В то время как The @ Company фокусируется на новом протоколе для безопасного обмена информацией, другие примеры включают Mozilla и Brave на стороне браузера, Neeva и DuckDuckGo в поиске и Linktree и Mastodon в социальных сетях, отметил Таллент.

«Соблюдение конфиденциальности - это, по сути, проблема, которую невозможно решить на уровне приложения / процесса, и она обычно не связана с хорошим онлайн-опытом», - отметила она.

Многих не волнует слежка, но они просто еще не знают, что есть лучший способ. Задача состоит в том, чтобы доказать, что это может быть фундаментально решено с помощью нового протокола / платформы, что возможны превосходные возможности, ориентированные на конфиденциальность, и засеять рынок этим лучшим опытом в Интернете, сотрудничая с разработчиками приложений.

«Мы (The @ Company) легко разбираемся в разработчиках приложений не только потому, что мы упрощаем интеграцию соблюдения конфиденциальности, но и потому, что наша платформа обеспечивает совершенно новый и лучший онлайн-опыт», - сказала она.

Типичный потребитель думает не о конфиденциальности, а об удобстве, информации, вдохновении и развлечениях при использовании Интернета. «Даже если безопасность или конфиденциальность становятся проблемой, типичный потребитель может не действовать, чтобы заменить решение, пока боль от неудобства или плохого опыта не превзойдет положительный опыт», - пояснил Таллент.

«Поэтому вместо того, чтобы ждать Интернет-Армагеддона, мы предпочитаем предоставлять пользователям опыт, который соответствует и, надеюсь, превосходит то, что люди в настоящее время получают от действующих поставщиков служебных приложений. Мы обнаружили, что игроки,

ориентированные на конфиденциальность, которые получают значительную поддержку, создали сильные «мосты». опыт, который позволяет людям попробовать альтернативу», - предложила она.

Если объединяющие возможности оправдают ожидания относительно хорошего пользовательского опыта, некоторые из них мгновенно выиграют. Но большинство из них со временем будут постепенно интегрироваться, пока они полностью не заменят свое предыдущее приложение альтернативным». ***(Jack M. Germain. How Fixable Is the Unsafe Internet? // TechNewsWorld (https://www.technewsworld.com/story/87097.html). 15.04.2021).***

***

«Технологический университет Суинберна подтвердил, что личная информация о сотрудниках, студентах и сторонних организациях случайно попала в открытый доступ.

В прошлом месяце было сообщено, что в Интернете доступна информация примерно о 5200 сотрудников Суинберна и 100 студентов Суинберна.

Эти данные, как сказал Суинберн, были регистрационной информацией о нескольких мероприятиях, начиная с 2013 года. Веб-страница регистрации на мероприятие больше не доступна.

Предоставляемая информация включала имя, адрес электронной почты и, в некоторых случаях, номер контактного телефона.

«Мы приняли немедленные меры для расследования и реагирования на эту утечку данных, включая удаление информации и проведение аудита на других подобных сайтах», - говорится в заявлении университета в пятницу.

«Мы искренне приносим свои извинения всем, кого затронула эта утечка данных, и за любые опасения, которые она вызвала».

Суинберн сказал, что в настоящее время он связывается со всеми людьми, чья информация была предоставлена, чтобы извиниться перед ними и предложить соответствующую поддержку.

«Мы также связываемся с примерно 200 другими людьми, не связанными с Суинберном, которые зарегистрировались для участия в мероприятии и чья информация также стала доступной», - говорится в сообщении.

О нарушении было сообщено в Управление комиссара по информации Австралии (OAIC), Управление комиссара по информации штата Виктория (OVIC), Агентство качества и стандартов высшего образования (TESQA) и Департамент образования штата Виктория.

Сектор высшего образования в Австралии вскоре может оказаться системой национального значения, поскольку правительство готово ввести в действие «усиленную основу для повышения безопасности и устойчивости» университетов через закон 2020 года о поправках к законодательству о безопасности (критическая инфраструктура).

Группа восьми (Go8), в которую входят восемь австралийских университетов, считает, что правительство на самом деле еще не определило какие-либо критически важные инфраструктурные активы в секторе высшего образования и исследований и, следовательно, не считает, что высшее образование

и исследования должны быть включены в эту категорию. сектор критической инфраструктуры с учетом нормативных разветвлений.

«Go8 считает, что всеобъемлющий характер законодательства, предложенного для сектора высшего образования и научных исследований, крайне непропорционален вероятной степени и степени критичности этого сектора», - говорится в сообщении в феврале.

Go8 состоит из Университета Аделаиды, Австралийского национального университета, Университета Мельбурна, Университета Монаша, Университета штата Вашингтон в Сиднее, Университета Квинсленда, Университета Сиднея и Университета Западной Австралии.

Суинберн представил свое собственное мнение комитету, исследующему законопроект, в феврале, заявив, что университетам будет трудно покрыть стоимость положительных обязательств по обеспечению безопасности и усиленных мер кибербезопасности для активов, которые считаются системами национального значения, учитывая текущую ситуацию с финансированием и снижение доходов от набора иностранных студентов.

«Поэтому Содружество должно гарантировать, что университеты получают адекватное финансирование, чтобы выполнять свои обязанности по обеспечению качественного образования и отвечать этим новым требованиям безопасности», - написано в [PDF].

«В то время как безопасность от иностранного вмешательства имеет первостепенное значение, не менее важна экономическая безопасность, обеспечиваемая надежным третичным сектором. Мы рекомендуем правительству тесно сотрудничать с этим сектором, чтобы обеспечить минимальное влияние законодательства на жизненно важные операции университетов».

В конце 2018 года Австралийский национальный университет (ANU) подвергся серьезной утечке данных, которая была обнаружена в мае 2019 года и обнаружена двумя неделями позже, в июне.

Хакеры получили доступ к данным за 19 лет в системе, в которой находятся кадры университета, управление финансами, администрация студентов и «корпоративные системы электронных форм».

Затем был университет RMIT в Мельбурне, который в феврале отреагировал на сообщения о том, что стал жертвой фишинг-атаки, заявив, что восстановление его систем медленно продвигается.

На недавних слушаниях в Объединенном парламентском комитете по разведке и безопасности (PJCIS) о рисках для национальной безопасности, влияющих на австралийский сектор высшего образования и исследований, представители Министерства внутренних дел использовали дискуссии вокруг двух инцидентов безопасности, чтобы оправдать включение высшего образования и исследований в законопроект о критической инфраструктуре.

АВСТРАЛИЯ ТАКЖЕ ОБВИНЯЕТ РОССИЮ В ВЗЛОМЕ SOLARWINDS

В другом месте, правительство Австралии присоединилось к международным партнерам холдинга России на счет своей кибер - кампанию против программного обеспечения американской фирмы, SolarWinds.

По данным США и Великобритании, хакеры, работающие на российскую службу внешней разведки, стоят за атакой SolarWinds, кампаниями кибершпионажа, нацеленными на исследовательские центры COVID-19, и многим другим.

Обвинение США содержится в совместном сообщении Агентства национальной безопасности, Агентства по кибербезопасности и безопасности инфраструктуры и Федерального бюро расследований, в котором также описывается текущая эксплуатация Службой внешней разведки России пяти общеизвестных уязвимостей в VPN-сервисах.

Великобритания также приписывает атаки российской разведке.

«В консультации с нашими партнерами правительство Австралии определило, что российские государственные субъекты активно используют SolarWinds и ее цепочки поставок», - говорится в заявлении министра иностранных дел Мариз Пейн, министра обороны Питера Даттона и министра внутренних дел Карен Эндрюс.

«За последние 12 месяцев Австралия стала свидетелем того, как Россия использовала злонамеренные действия для подрыва международной стабильности, безопасности и общественной безопасности. Австралия осуждает такое поведение».

Атаки на цепочки поставок, нацеленные на компанию SolarWinds, производящую программное обеспечение для управления ИТ, представляли собой один из крупнейших инцидентов в области кибербезопасности за последние годы, когда хакеры получили доступ к сетям десятков тысяч организаций по всему миру, включая несколько правительственных агентств США, а также компаний, занимающихся кибербезопасностью.

«Российская кампания затронула тысячи компьютерных систем по всему миру. Австралия признает высокие затраты, которые несет частный сектор США», - говорится в заявлении Австралии». ***(Asha Barbaschow. Swinburne University confirms over 5,000 individuals affected in data breach // ZDNet (https://www.zdnet.com/article/swinburne-university-confirms-over-5000-individuals-affected-in-data-breach/). 16.04.2021).***

***

«В среду эксперты по безопасности данных подвергли сомнению заявление Facebook о том, что данные полумиллиарда пользователей, обнаруженных в Интернете, являются общедоступной информацией профилей пользователей.

После того, как за выходные были обнаружены 533 миллиона записей пользователей Facebook, включая номера телефонов, идентификаторы Facebook, полные имена и даты рождения, компания, занимающаяся социальными сетями, в одночасье выступила в защиту, заявив, что информация в базе данных, которая распространяется в Интернете, является общедоступной.

«Важно понимать, что злоумышленники получили эти данные не путем взлома наших систем, а путем очистки их с нашей платформы до сентября 2019 года. Очистка - это распространенная тактика, которая часто использует

автоматизированное программное обеспечение для извлечения общедоступной информации из Интернета», - заявление гласит.

Но эксперты по безопасности данных заявили, что защита социальной сети уклончива.

«Заявление Facebook о том, что эта информация является общедоступной, вводит в заблуждение, поскольку это нарушение также включает номера телефонов, которые не были видны в профилях людей», - сказал Инти Де Сеукелайр, бельгийский этический хакер.

Независимый исследователь кибербезопасности Лукаш Олейник также подверг сомнению позицию Facebook.

«Это действительно общедоступные данные? Например, телефонные номера, по крайней мере, во многих случаях, не были, и были получены из Facebook», - сказал он.

Утечка сосредоточена вокруг функции импорта контактов, что означало, что пользователей по-прежнему можно было обнаружить по их номерам телефонов, даже если номер не был публично указан в их профиле - проблема, которую Де Сеукелайр поднял еще в 2017 году.

Facebook обвинил в утечке злоупотребление этой функцией сопоставления, заявив, что обновил эту функцию в 2019 году после того, как обнаружил, что злоумышленники злоупотребляли ошибкой в программном обеспечении функции, чтобы сопоставить пачки телефонных номеров с пользователями Facebook для создания базы данных.

Но предложение Facebook о том, чтобы номера телефонов были общедоступными, потому что их можно было использовать для сопоставления пользователей, даже если соответствующие номера телефонов не были публично указаны, было поставлено под сомнение.

Бывший чиновник Федеральной торговой комиссии США Ашкан Солтани написал в Твиттере, что из двух его телефонных номеров, которые появились в утечке, один был виден только ему, а другой был «более чувствительным» номером, используемым для восстановления учетной записи и сброса паролей.

Майкл Вел, британский ученый-компьютерщик, сообщил, что его номер появился в утечке, хотя все его настройки конфиденциальности были на максимальном уровне.

«Даже если пользователи поставят галочку в поле, говоря, что друзья могут найти их по их телефонному номеру, это не задача тех же пользователей, чтобы представить, как эта система может быть использована в больших масштабах, чтобы сделать эти телефонные номера общедоступными, прежде чем сделать этот выбор. работа Facebook ", - сказал Вил».

«Если Facebook не может сделать такую систему безопасной, им не следовало ее внедрять». ***(VINCENT MANANCOURT. 'Misleading' Facebook data leak claims questioned // POLITICO (https://www.politico.eu/article/facebook-data-leak-misleading-claims-questioned/). 07.04.2021).***

***

«Ирландская комиссия по защите данных в среду начала расследование в отношении Facebook после того, как в сети появились данные о более чем полмиллиарда пользователей платформы.

Множество данных, в том числе номера телефонов, идентификаторы Facebook, полные имена и даты рождения, были обнаружены Алоном Галом из разведывательной компании Hudson Rock в этом месяце после того, как они были размещены в Интернете бесплатно.

В сегодняшнем заявлении Комиссия по защите данных (DPC) заявила, что начинает расследование, поскольку считает, что Facebook, возможно, нарушил Общие правила защиты данных ЕС. Фирма, занимающаяся социальными сетями, отрицает это.

«DPC, рассмотрев информацию, предоставленную Facebook Ирландия по этому поводу на сегодняшний день, считает, что одно или несколько положений GDPR... могли быть и / или нарушаются в отношении пользователей Facebook» личные данные."

После новостей о том, что было обнаружено хранилище данных 533 миллионов пользователей, Facebook сначала заявил, что это старые данные, о которых ранее сообщалось в 2019 году. «Мы обнаружили и исправили эту проблему в августе 2019 года», - написала в Twitter представитель Facebook Лиз Буржуа.

Затем 6 апреля компания опубликовала заявление, в котором пояснила, что база данных состоит из информации, извлеченной из общедоступных профилей, и что она устранила проблему, которая позволила очистить данные в 2019 году.

«Важно понимать, что злоумышленники получили эти данные не путем взлома наших систем, а путем очистки их с нашей платформы до сентября 2019 года. Очистка - это распространенная тактика, которая часто использует автоматизированное программное обеспечение для извлечения общедоступной информации из Интернета», - компания сказала». ***(VINCENT MANANCOURT. Ireland to probe Facebook following massive data leak // POLITICO (https://www.politico.eu/article/ireland-to-probe-facebook-following-massive-data-leak/). 14.04.2021).***

***

«Разработчик комплектов Wi-Fi Ubiquiti предположил, что злоумышленник, который получил доступ к некоторым из его облачных систем в январе 2021 года, мог уйти с исходным кодом и логинами сотрудников, а не с данными клиентов, о которых он изначально предупреждал, могут оказаться в опасности.

Новости о взломе облачных серверов Ubiquiti появились 11 января 2021 года, когда компания отправила клиентам по электронной почте текст из этого сообщения на форуме поддержки. В этом послании говорилось: «Недавно нам стало известно о несанкционированном доступе к некоторым нашим системам информационных технологий, размещенным сторонним поставщиком облачных услуг».

Это объявление продолжалось: «У нас нет никаких указаний на несанкционированную активность в отношении учетной записи любого пользователя», но также рекомендовалось клиентам изменить свои пароли, потому что, если к их записям был осуществлен доступ, хэшированные и соленые пароли, адреса электронной почты и даже физические адреса и номера телефонов могут оказаться под угрозой.

В обновленной информации, опубликованной в среду на этой неделе, говорится, что расследование, проведенное внешними экспертами, «не выявило доказательств того, что к информации о клиентах был осуществлен доступ или что она была направлена против нее».

Важно отметить, что обновление также показало, что кто-то «безуспешно пытался вымогать у компании деньги, угрожая раскрыть украденный исходный код и определенные учетные данные ИТ». Обновление не предполагает, что попытка вымогательства была надуманной.

Ubiquiti не сообщила, когда внешние эксперты решили, что данные о клиентах остались нетронутыми. Это оставляет компанию в интересном положении, поскольку она, возможно, знает, что ее основной IP-адрес просочился, и не раскрывает это, а также знает, что данные клиентов находятся в безопасности, и не раскрывает это.

Обновление содержит еще один пугающий самородок в этом предложении: «Обратите внимание, что с момента нашего уведомления от 11 января ничего не изменилось в отношении нашего анализа данных клиентов и безопасности наших продуктов».

Но в уведомлении от 11 января не упоминается «безопасность наших продуктов».

Обновление в среду было опубликовано через два дня после того, как Krebs On Security сообщила, что увидела письмо осведомителя в Европейский надзорный орган по защите данных, в котором утверждается, что Ubiquiti не рассказала всю правду об инциденте.

Кребс сказал, что в письме атака на Убиквити описывалась как «катастрофически хуже, чем сообщалось».

«Нарушение было массовым, данные клиентов оказались под угрозой, доступ к устройствам клиентов, развернутым в корпорациях и домах по всему миру, был под угрозой», - сообщается в письме, добавляя, что команда юристов Ubiquiti «подавила и отвергла усилия по решительной защите клиентов.»

Информатор отдельно утверждал, что кто бы ни смог взломать серверы Ubiquiti, размещенные на Amazon, они могли украсть криптографические секреты для файлов cookie единого входа клиентов и удаленного доступа к устройствам, внутреннего исходного кода и ключей подписи - гораздо больше, чем Wi-Fi. Производитель Fi Box раскрыт в январе. Утверждается, что злоумышленник получил привилегированные учетные данные ИТ-специалиста Ubiquiti, получил root-доступ к корпоративным системам AWS и, таким образом, потенциально мог бесплатно использовать свое облачное хранилище и базы данных.

Бэкдоры, по-видимому, тоже были спрятаны на серверах, и, как Ubiquiti признал на этой неделе, потребовали выкуп, чтобы не говорить о взломе.

Если бы учетные данные сотрудников Ubiquiti были получены, как теперь предполагает даже сама Ubiquiti, злоумышленники могли бы с комфортом получить «доступ к устройствам клиентов, развернутым в корпорациях и домах по всему миру», как говорится в письме информатора.

Правильные кредиты также могут подвергнуть данные клиентов риску кражи. На этой неделе Ubiquiti настаивала на том, что злоумышленники не «получали доступ и даже не нацеливались» на такие данные, хотя информатор утверждал, что производитель беспроводных комплектов вел недостаточные журналы, чтобы быть уверенным в этом.

В сообщении Ubiquiti в среду говорилось: «На данный момент у нас есть хорошо разработанные доказательства того, что злоумышленник является человеком со сложными знаниями о нашей облачной инфраструктуре», но сказал, что не может сказать больше из-за продолжающихся расследований.

Подводя итог: исходный код продуктов Ubiquiti и другая внутренняя информация, возможно, были отфильтрованы, серверы могли быть рутированы, и кто-либо ответственный может быть текущим или бывшим сотрудником компании... но, кроме нескольких случайных слов, Ubiquiti имеет выбран, чтобы сосредоточиться на проблеме личной конфиденциальности, он говорит, что на самом деле это не проблема.

И все это произошло в то время, когда мы знаем, что злоумышленники могли годами скрывать свое присутствие в инфраструктуре SolarWinds и отравлять ее продукты.

Обновление заканчивается еще одним призывом к клиентам обновить свои пароли и включить двухфакторную аутентификацию. Регистр считает, что некоторые читатели также могут подумать об обновлении своего поставщика Wi-Fi». ***(Simon Sharwood. Wi-Fi slinger Ubiquiti hints at source code leak after claim of 'catastrophic' cloud intrusion emerges // The Register (https://www.theregister.com/2021/04/01/ubiquiti_data_breach/). 01.04.2021).***

***

«Онлайн-платформа Codecov для отчетов и статистики размещенного тестирования кода объявила в четверг, что злоумышленник изменил свой сценарий Bash Uploader, раскрывая конфиденциальную информацию в среде непрерывной интеграции (CI) клиентов.

Компания узнала о компрометации 1 апреля, но расследование установило, что первые признаки атаки на цепочку поставок программного обеспечения произошли в конце января.

Изменения в Bash Uploader начались в январе

Codecov предоставляет инструменты, которые помогают разработчикам измерить, какая часть исходного кода выполняется во время тестирования, процесс, известный как покрытие кода, которое указывает на возможность появления необнаруженных ошибок в коде.

Клиентская база компании насчитывает более 29 000 предприятий, включая Atlassian, Washington Post, GoDaddy, Royal Bank of Canada и Procter & Gamble.

Как следует из названия, Bash Uploader - это инструмент, который клиенты Codecov используют для отправки отчетов о покрытии кода на платформу. Он обнаруживает специфические настройки CI, собирает отчеты и выгружает информацию.

Начиная с 31 января злоумышленники сосредоточили свое внимание на этом инструменте сбора данных. Они изменили сценарий, чтобы доставлять детали из среды клиентов на сервер за пределами инфраструктуры Codecov, который отображается в строке 525.

Слабым местом, использованным для получения доступа, была ошибка в процессе создания образа Docker Codecov, которая позволяла извлекать учетные данные, защищающие модификацию сценария Bash Uploader.

Учитывая информацию, собранную Bash Uploader, Codecov говорит, что злоумышленник мог использовать вредоносную версию для экспорта следующих конфиденциальных данных:

Любые учетные данные, токены или ключи, которые наши клиенты передавали через свой исполнитель CI, которые будут доступны при выполнении скрипта Bash Uploader.

Любые службы, хранилища данных и код приложения, к которым можно получить доступ с помощью этих учетных данных, токенов или ключей.

Удаленная информация git (URL-адрес исходного репозитория) репозиториев, использующих загрузчики Bash для загрузки покрытия в Codecov в CI.

Из-за этого потенциального риска затронутым пользователям настоятельно рекомендуется повторно запустить все учетные данные, токены или ключи, присутствующие в переменных среды в процессах CI, которые полагались на Bash Uploader.

Клиенты, использующие локальную версию сценария, должны проверить, существует ли код злоумышленника, добавленный в строке 525. Если приведенный ниже код присутствует, они должны заменить файлы bash последней версией скрипта Codecov.

В исходном варианте скрипт выгружает данные из переменной «ENV» на платформу Codecov. После того, как злоумышленник изменил его, Bash Uploader также отправлял данные по указанному выше адресу, IP от Digital Ocean, который не находился под управлением Codecov.

Codecov узнал о компрометации от клиента, который заметил, что значение хеш-функции для сценария Bash Uploader на GitHub не соответствует значению для загруженного файла.

Сразу после обнаружения компрометации компания предприняла шаги по смягчению последствий инцидента, которые включали следующее:

ротация всех соответствующих внутренних учетных данных, включая ключ, используемый для облегчения модификации Bash Uploader

аудит, где и как был доступен ключ

настройка инструментов мониторинга и аудита, чтобы гарантировать, что такого рода непреднамеренные изменения не могут снова произойти в Bash Uploader

работа с хостинг-провайдером стороннего сервера, чтобы убедиться, что вредоносный веб-сервер был должным образом выведен из эксплуатации

Codecov сообщает, что инцидент произошел, несмотря на установленные политики, процедуры, методы и средства контроля безопасности, а также постоянный мониторинг сети и систем на предмет необычной активности». ***(Ionut Ilascu. Popular Codecov code coverage tool hacked to steal dev credentials // Bleeping Computer (https://www.bleepingcomputer.com/news/security/popular-codecov-code-coverage-tool-hacked-to-steal-dev-credentials/). 16.04.2021).***

***

«Компания Belden сообщила, что в ходе кибератаки в ноябре 2020 года были получены и скопированы дополнительные данные, связанные с медицинскими льготами сотрудников и членами их семей, подпадающими под их план.

Belden - американский производитель устройств для подключения к сети, включая маршрутизаторы, межсетевые экраны, коммутаторы, кабели и разъемы. Выручка Belden за 2019 год составила 2,5 миллиарда долларов, в компании работает около 9000 человек.

В ноябре 2020 г. Компания Belden сообщила, что они подверглись кибератаке, в ходе которой злоумышленники получили доступ и скопировали «некоторые текущие и бывшие данные сотрудников, а также информацию ограниченной компании о некоторых деловых партнерах».

В опубликованном вчера новом сообщении Belden говорится, что расследование показало, что злоумышленники получили доступ к дополнительным данным во время этой атаки.

Эти данные принадлежат супругам, иждивенцам и родственникам нынешних и бывших сотрудников Belden, которые получили медицинскую страховку от компании.

«Помимо хранения личной информации некоторых нынешних и бывших сотрудников, мы впоследствии узнали, что затронутые серверы также содержали некоторую личную информацию некоторых супругов, иждивенцев и родственников некоторых нынешних и бывших сотрудников. Кроме того, 9 февраля 2021 года или после этой даты мы узнали, что информация, раскрытая в ходе инцидента, также включала информацию, связанную со здоровьем», - сообщил вчера Белден.

Belden заявляет, что информация, связанная со здоровьем, включает имена людей, пол, информацию о льготах, номера групп, покрытие и их отношение к сотруднику.

Компания заявляет, что они не верят, что украденные данные включали какую-либо информацию, касающуюся состояния здоровья или диагнозов, в доступные данные.

Belden начала рассылать уведомления тем, кого затронуло это последнее раскрытие, которое содержит бесплатный мониторинг личности жертв.

Природа кибератаки Belden в 2020 году так и не была раскрыта, но, скорее всего, это была атака с использованием программ-вымогателей.

Во время атак программ-вымогателей злоумышленники обычно крадут незашифрованные файлы перед шифрованием устройств в сети. Затем злоумышленники предупреждают жертву, что они опубликуют украденные данные на сайтах утечки данных, если выкуп не будет уплачен.

Неизвестно, заплатила ли Belden выкуп в рамках своей кибератаки, но на данный момент ни один злоумышленник не опубликовал свои данные». ***(Lawrence Abrams. Belden says health benefits data stolen in 2020 cyberattack // Bleeping Computer (https://www.bleepingcomputer.com/news/security/belden-says-health-benefits-data-stolen-in-2020-cyberattack/). 08.04.2021).***

***

«База данных социальной сети Clubhouse, содержащая персональную информацию 1,3 миллиона пользователей, была опубликована на популярном хакерском форуме.

Среди данных, которые оказались доступны в сети, такая информация как ID пользователя, его имя и никнейм, аккаунты в Twitter и Instagram, связанные с основным профилем, количество подписчиков и людей, на которых подписан пользователь, дата создания аккаунта, имя пригласившего пользователя.

База данных содержит только информацию профиля Clubhouse — среди опубликованной информации нет данных кредитных карт или юридических документов.

Clubhouse не прокомментировал утечку данных оперативно.

Хакеры могут использовать данные несколькими способами, пишет CyberNews. Во-первых, они могут провести целенаправленные атаки. Во-вторых — подбирать пароли к профилям Clubhouse и взламывать аккаунты.

Исследователи безопасности сообщили Business Insider, что хакеры могут использовать открытые данные, чтобы выдать себя за пользователей или обманным способом заставить их раскрыть конфиденциальную информацию для входа в аккаунты.

Аналитик разведывательной компании IntSights Пол Прюдомм сказал Business Insider, что раскрытие данных имеет большое значение, поскольку злоумышленники могут использовать их для атак на компании через информацию сотрудников.

CyberNews предлагает проверить утечку данных с помощью собственного сервиса, который изучает утечки на основе данных электронной почты. CyberNews также рекомендует пользователям Clubhouse изменить пароль учетной записи и использовать диспетчер паролей, включить двухфакторную аутентификацию для аккаунтов во всех соцсетях и остерегаться потенциальных фишинговых писем и текстовых сообщений, не отвечать незнакомым людям.

Несколько дней назад в интернете выставили на продажу данные более миллиарда профилей Facebook и LinkedIn». ***(Виктория Сафронова. Личные данные 1,3 млн пользователей Clubhouse оказались в открытом доступе // ООО "РБ.РУ" (https://rb.ru/news/lichnye-dannye-clubhouse/). 11.04.2021).***

***

«В открытом доступе оказались данные электронных адресов пользователей сайта-карты Навального.

Неизвестные хакеры слили в Сеть базу электронных адресов потенциальных участников оппозиционных митингов, зарегистрированных на сайте «Свободу Навальному». В ней почти 530 тысяч аккаунтов, при этом 70% из них — боты.

Сообщение от директора Фонда появилось в ТГ-канале «Команда Навального». По словам Жданова, база полностью соответствует действительности и не является фейком.

«Мы видим, что это база, которая используется нами для рассылки по электронным адресам. Для рассылки по электронным почтам мы используем сторонние сервисы, — подчеркнул Жданов. — Это исключительно база электронных адресов, без фамилий, имен или каких-либо уточняющих данных. Самую большую подлость, которую могут сделать злоумышленники — отправить вам неприятное письмо, которое, вероятно, попадет в спам».

Однако директор Ассоциации профессиональных пользователей сетей и мессенджеров Владимир Зыков опроверг его слова, отметив, что они не соответствуют действительности, пишет Федеральное агентство новостей (ФАН).

Эксперт подчеркнул, что другие подобные случаи показывали на практике, что после утечки можно узнать о человеке все, включая место проживания и номер телефона. Хакеры, по словам Зыкова, при желании смогут деанонимизировать людей, зарегистрировавшихся на сайте-карте блогера». ***(Данные сторонников Навального утекли в Сеть // SecurityLab.ru (https://www.securitylab.ru/news/519011.php). 16.04.2021).***

***

«В открытом доступе оказалась полная база данных мобильного приложения Elector, использовавшегося для регистрации избирателей на парламентских выборах в Израиле, которые прошли 23 марта 2021 марта. Как в среду, 14 апреля, сообщил Telegram-канал «Утечки информации», об инциденте стало известно в конце прошлого месяца.

База данных содержит информацию 6,5 млн пользователей, в том числе имена и фамилии, номера удостоверений личности, адреса, номера телефонов (не для всех избирателей), электронные адреса (не для всех избирателей), даты рождения и сведения о половой принадлежности.

Это уже не первая утечка данных израильских избирателей. В феврале 2020 года израильская партия «Ликуд» загрузила весь реестр избирателей страны в приложение Elector, в котором содержались опасные уязвимости. В течение нескольких дней персональные данные почти 6,5 млн избирателей, в том числе ведущих израильских политиков, находились в открытом доступе. База данных содержала имена, адреса, серии и номера документов, а также сведения о политических предпочтениях. Любой пользователь мог получить доступ к информации через web-браузер без использования каких-либо инструментов». ***(В Сеть утекли данные 6,5 млн израильских избирателей // SecurityLab.ru (https://www.securitylab.ru/news/518858.php). 14.04.2021).***

***

«Специалисты международного разработчика антивирусного программного обеспечения, эксперта в области киберзащиты – компании ESET рассказали, как сократить утечку личных данных интернет-пользователей, таких как: информации в соцсетях, электронных письмах и мессенджерах, информации об онлайн-платежах, истории местоположений, чтобы они не попали в руки злоумышленников.

Как сообщают в компании ESET, перечисленные виды информации – это лишь часть данных, которые составляют цифровой след каждого человека. Полнота этого цифрового портрета зависит от конкретных привычек распространения личной информации и отношения к конфиденциальности интернет-пользователя.

"Значительная часть ваших данных может быть использована киберпреступниками во вредоносных целях или продана на черных рынках. Даже если вы считаете, что ваши данные никого не интересуют, в интернете жертвой киберпреступников может стать каждый. Однако, хорошая новость заключается в том, что существует достаточно много способов уменьшения своего цифрового следа. Наличие рисков вовсе не означает, что стоит перестать использовать интернет-сервисы, но необходимо соблюдать баланс между приватностью и удобством", - сообщили в компании ESET.

Конфиденциальность в социальных сетях

Согласно сообщению, первый шаг в уменьшении цифрового следа - это проверка основных настроек конфиденциальности в соцсетях: кто именно может просматривать ваши публикации и личные данные и сколько информации они могут видеть. Далее необходимо очистить список друзей: начните с удаления из друзей всех незнакомцев, которых вы даже не помните, а затем переходите к знакомым, которых вы не очень хорошо знаете, а также к людям, с которыми перестали общаться.

"Если вы думаете "какая разница, кто видит мои публикации?", на самом деле это имеет большое значение. Из ваших социальных сетей можно получить много информации, которую затем можно использовать во вредоносных целях", - подчеркнули в ESET.

Например, известно много случаев, когда мошенники собирали информацию о привычках знаменитостей, отслеживая их аккаунты в Instagram, чтобы ограбить их дома.

Проверка посещаемых сайтов

Большинство людей имеют десятки, а может и сотни различных аккаунтов в интернете - различные веб-сайты для покупок, фитнес-приложения, кулинарные сайты, игры и многие другие. Как отмечают в ESET, каждый из этих сайтов и приложений сохраняет различные типы конфиденциальной информации, которая может заинтересовать злоумышленников, в частности имя, дату рождения и номер телефона.

Чтобы облегчить процесс регистрации, сегодня доступна технология единого входа через учетные записи Google, Facebook или Apple. И поскольку почти никто не имеет полного списка всех сайтов, магазинов и приложений, в которых регистрировался в течение многих лет, опция единого входа может пригодиться.

Независимо от того, какой именно аккаунт вы использовали, все они дают возможность выяснить, какие сторонние программы имеют к нему доступ.

Отмена подписок на рассылки

Как добавляют специалисты по кибербезопасности, еще один способ уменьшить свой цифровой след - это отмена подписок на электронные рассылки новостей, которые вы получаете. Многие подписки подключаются автоматически при создании учетных записей в различных сервисах и интернет-магазинах, которые затем отправляют вам электронные письма с новостями и различными предложениями скидок на товары и услуги.

Большинство людей не читают мелкий шрифт при регистрации, а просто автоматически все подтверждают, чтобы быстрее ее закончить. Поэтому в конечном итоге такие пользователи имеют сотни непрочитанных рекламных писем.

"После очистки почты от ненужных подписок, разумным шагом будет создание отдельного адреса электронной почты, который будет использоваться для покупок", - советуют в компании ESET.

При этом, эксперты подчеркнули, что процесс минимизации цифрового следа не ограничивается упомянутыми выше шагами. Еще одним важным инструментом для уменьшения цифрового следа является виртуальная частная сеть (VPN), которая работает как зашифрованный туннель для вашего интернет-трафика и защищает вас от отслеживания.

"Вы также можете использовать проверку конфиденциальности Google и другие инструменты, чтобы увидеть, какие данные сервис сохраняет и прекратить это по мере необходимости. Кроме этого, если вам интересно узнать, какую информацию о вас имеет Twitter или Facebook, вы можете скачать копию всех данных, которую они хранят", - добавили в ESET…». ***(Специалисты по кибербезопасности дали советы, как сократить утечку личных данных в интернете // УНИАН (https://www.unian.net/science/kiberbezopasnost-specialisty-dali-sovety-kak-sokratit-utechku-lichnyh-dannyh-v-internete-novosti-11390803.html). 16.04.2021).***

***

«26 апреля 2021 года Судебная палата Бельгийского управления по защите данных (BDPA) наложила свой первый штраф специально за сбои в кибербезопасности.

Это решение следует за другими решениями, в которых Судебная палата рассматривала нарушения кибербезопасности в качестве одного из факторов (см., Например, решение от 22 января 2021 г.), и это должно служить сигналом для других организаций: все контроллеры и процессоры должны гарантировать, что технические и организационные меры, которые они приняли для защиты персональных данных, являются надлежащими. В противном случае счет может быть на порядок выше затрат на реализацию таких мер. Штрафы в Европейском Союзе и в Соединенном Королевстве за нарушения кибербезопасности часто составляют сотни тысяч или даже миллионы евро, причем более ограниченные штрафы (например, этот, в размере 100000 евро) часто связаны с тем, что можно рассматривать как ограниченное. нарушения кибербезопасности - или

ограниченное количество известных затронутых субъектов данных. Если организация терпит неудачу в обеспечении кибербезопасности, может быть наложен крупный штраф.

Иными словами, кибербезопасность - это не невозвратные затраты, а хорошее и необходимое вложение. Это важная гарантия для бизнеса, во многих случаях аргумент в пользу продаж, но также отличный способ ограничить стоимость (неизбежных) инцидентов и уменьшить штрафы за неадекватные меры.

А) Факты: ограниченный доступ, но нет возможности проверить правильность использования

Рассматриваемый случай касался доступа финансового учреждения к Центральному кредитному регистру, управляемому Национальным банком Бельгии. Согласно тексту решения, рассматриваемое финансовое учреждение предоставило сотрудникам два способа доступа к реестру в зависимости от их стажа (один для штатных сотрудников, а другой для менеджеров). Первый метод зарегистрировал, кто использовал рассматриваемую систему. Один для менеджеров - нет; по данным финансового учреждения, (только) пять человек имели доступ к реестру таким образом - все с одним и тем же паролем.

СОВЕТ: Если в вашей организации используется аналогичный подход, может потребоваться его переоценка. Если один уникальный пароль дает доступ к системе и личность пользователя зарегистрирована, вы не будете знать, кто именно использует систему - кто из авторизованных пользователей, но также и то, является ли он авторизованным пользователем или неавторизованным пользователем.

В данном конкретном случае одно или несколько из пяти рассматриваемых лиц обращались к досье женщины в реестре не менее 20 раз в течение двух лет. Однако из-за отсутствия какой-либо регистрации того, какие лица имели доступ к реестру в каждый из этих периодов, было невозможно определить, кто именно это сделал.

Факты предполагают простой ответ, поскольку в то время бывший муж женщины был среди пяти упомянутых лиц, и они с ней находились в процессе ликвидации своего совместного имущества после развода. Женщина подозревала, что бывший муж использовал этот доступ к базе данных для получения информации, которая затем дала ему преимущество в процессе ликвидации, и подала отдельную жалобу в БДПА против него индивидуально. На сегодняшний день решение по этому поводу не опубликовано.

СОВЕТ: Знаете ли вы, что доступ авторизованного пользователя в неавторизованных целях (например, злоупотребление правами доступа) может рассматриваться как «злоупотребление доверием» в соответствии с нормами уголовного права? Всегда учитывайте это, а также последствия трудового законодательства, если есть необходимость подать собственную жалобу (например, если это требуется в соответствии с вашим страховым полисом).

Таким образом, жалоба на финансовое учреждение была сосредоточена не на том, было ли это умышленное нарушение закона о защите данных бывшим мужем, а на том, приняло ли финансовое учреждение соответствующие меры для «обеспечения уровня безопасности, соответствующего риску», в соответствии с требованиями статьи 32 Общего регламента по защите данных или GDPR.

Б) Отсутствие логирования = вопиющее нарушение?

По мнению Судебной палаты, «отсутствие какой-либо системы контроля доступа менеджеров» в данном случае было «вопиющим нарушением» статьи 32 GDPR, в частности потому, что данные, доступные через систему, были «конфиденциальными финансовыми данными». Такой характер означал, что риски для основных прав субъектов данных были высоки, поэтому принимаемые меры должны были быть «тем более уместными».

Отсутствие ведения журнала или других мер безопасности также рассматривалось как препятствие субъектам данных в использовании их права доступа в отношении (незаконной) обработки, поскольку финансовое учреждение не хранило никаких доказательств такой обработки.

СОВЕТ: Всегда думайте о более широких последствиях той или иной меры, прежде чем вводить ее в действие. Что касается журналов, например, для вашей организации нет юридического требования создавать и поддерживать журналы за любой заданный период времени (шесть месяцев, пять лет и т. Д.). Однако отсутствие ведения журнала может быть проблемой, как показано здесь, а слишком быстрое удаление журналов может привести к уничтожению полезных доказательств - даже если это было сделано по правильным причинам (например, во имя ограничения хранилища или минимизации данных).

Не все было плохо - были меры по ограничению доступа («всего» пять человек, позже - два человека). Однако Судебная палата сочла эти меры недостаточными, поскольку финансовое учреждение не могло контролировать, у кого был доступ, и соответствовал ли такой доступ целям, определенным учреждением.

Без надлежащих мер безопасности для обеспечения наличия и эффективности процедур контроля доступа сотрудников и руководителей к обрабатываемым данным Судебная палата обнаружила, что финансовое учреждение нарушило (i) свое обязательство по обеспечению безопасности обработки данных. деятельности (статья 32 GDPR), (ii) обязательство соблюдать принципы защиты данных намеренно и по умолчанию (статья 25 GDPR) и (ii) принцип подотчетности (статья 5 (2) и 24 GDPR).

С) Роли DPO и CISO могут быть совместимы, если они носят чисто рекомендательный характер.

БДПА ранее занимало позиции относительно роли DPO, которые регулярно комментировались во всем Европейском Союзе, в частности решение, в котором Судебная палата BDPA постановила, что «роль главы отдела [...] несовместима с ролью DPO». потому что DPO не может осуществлять какой-либо независимый надзор за таким отделом, даже если соответствующие отделы (например, риск) выполняли консультативную функцию.

В своем последнем решении Судебная палата, похоже, несколько смягчила свое видение, признав, что DPO в финансовом учреждении может сочетать роль DPO с ролью CISO (то есть главного сотрудника по информационной безопасности). Аргументация Судебной палаты состоит в том, что эта конкретная роль CISO является чисто консультативной:

директор по информационной безопасности «представляет руководству компании риски и их важность, и […] руководство должно решить, достаточны ли принятые меры для снижения рисков» ;

«В случае разногласий между [CISO] и руководством относительно принятых мер и несмотря на комментарии, представленные [руководству], это решение [CISO] не принимает»;

«Меры безопасности входят в компетенцию ИТ-отдела, а не директора по информационной безопасности».

Судебная палата здесь попыталась реклассифицировать свое предыдущее решение как то, в котором DPO «одновременно отвечал за различные операционные отделы», что, по-видимому, является искаженным видением предыдущего решения. В частности, нам неясно, почему к роли «Риск» из предыдущего решения следует относиться иначе, чем к роли «CISO», описанной в этом новом решении.

В любом случае, новая аргументация кажется более убедительной, чем предыдущая, и принесет утешение многим организациям, поскольку DPO совмещают консультативные роли, в особенности те, в которых DPO также действует как (советник) CISO.

Наконец, согласно этому новому решению, тот факт, что DPO ответил на жалобу, использовав слово «мы» для обозначения компании («мы, естественно, приняли меры», «мы извинились» и т. Д.), Не является нарушением. независимости ОИ. Это снова успокоит ряд организаций, но неясно, разделяет ли это позиция BDPA: мы видели случаи, когда собственная инспекционная служба BDPA ставила под сомнение независимость DPO клиента, отвечая «мы» в письме. По крайней мере, теперь такая критика не потребует длинных юридических аргументов для опровержения - достаточно простой ссылки на это конкретное решение.

Г) Результат: штраф и приказ соблюдать

На основании своих выводов о несоблюдении требований статьи 32 GDPR Судебная палата наложила штраф в размере 100 000 евро (второй по величине штраф на сегодняшний день в Бельгии после штрафа Google в размере 600 000 евро за право на забвение).

Помимо оборота финансового учреждения, на достижение этой суммы влияли различные факторы. Во-первых, обработанные данные считались конфиденциальными (финансовые данные, касающиеся кредитоспособности), что, как указывалось ранее, означало, что принятые меры должны быть «тем более уместными» из-за высоких рисков для основных прав человека. субъекты данных. Другие факторы включали (i) длительный период, в течение которого выполнялись операции обработки, (ii) большое количество операций обработки (20 раз для одного субъекта данных), (iii) ограниченное количество дополнительных мер. приняты после инцидента для усиления безопасности операций обработки и (iv) риска дальнейших незаконных операций обработки, если не было жалоб.

Здесь следует отметить один аспект, который может появиться снова, если финансовое учреждение обжалует решение, заключается в том, что период, охватываемый нарушением, начался задолго до того, как GDPR стал применяться: рассматриваемый «длительный период», принимаемый во внимание при

установлении суммы штраф продолжался с апреля 2016 года по август 2018 года; Аналогичным образом, похоже, что по крайней мере некоторые из 20 случаев доступа к данным субъекта данных предшествовали GDPR. В этих обстоятельствах кажется справедливым задаться вопросом, наложила бы ли Судебная палата штраф в размере 100000 евро, если бы она изучила случаи доступа только в период с 25 мая 2018 г. по август 2018 г.

E) Что происходит в других местах (власти Великобритании и ЕС)

Хотя размер штрафа может быть значительным по сравнению с предыдущими штрафами в Бельгии, он относительно невысок по сравнению со штрафами из других стран.

Частично это может быть связано с ограниченным объемом нарушения (только один известный случай из-за связи только с одной жалобой), но частично может иметь отношение к подходу каждого надзорного органа.

За пределами Бельгии некоторые из самых высоких штрафов, наложенных на сегодняшний день за нарушение GDPR, были напрямую связаны, по мнению соответствующих властей, с несоблюдением требований статьи 32 GDPR.

Например, в октябре 2020 года власти Великобритании, ICO (Управление комиссара по информации) наложили штрафы в размере 22 млн фунтов стерлингов и 20,5 млн фунтов стерлингов на British Airways и Marriott International соответственно за нарушения безопасности (первый за неспособность защитить личные и финансовые данные более 400 000 его клиентов после атаки на цепочку поставок; последнее - в результате недостаточного мониторинга привилегированных учетных записей, баз данных и отсутствия контроля над критически важными системами).

Шведский орган (Datainspektionen) также наложил в декабре 2020 года штраф в размере 3 миллионов евро на больницу Capio St Görans (i) за невыполнение анализа рисков перед предоставлением разрешения персоналу на доступ к картам пациентов и (ii) за отсутствие ограничения таких разрешений. к тому, что было строго необходимо пользователям для выполнения своих обязанностей. Кроме того, в августе 2019 года власти Болгарии наложили штраф в размере 2,6 миллиона евро на Национальное агентство по доходам (то есть налоговые органы) за отсутствие логического контроля доступа к личным данным 6 миллионов человек.

В Нидерландах также были наложены различные штрафы за нарушения кибербезопасности, с особым упором на больницы (штрафы в размере 440 000 евро и 460 000 евро в первую очередь).

Таким образом, в зависимости от того, как вы на это смотрите - в абсолютном выражении или как штраф, связанный с одним субъектом данных - этот бельгийский штраф может выглядеть как сделка (100000 евро против многомиллионных штрафов) или чрезвычайно дорогой штраф (размер штрафа British Airways до 55 фунтов стерлингов за каждого затронутого субъекта данных).

В любом случае, эта международная тенденция - наложение (высоких) штрафов за неадекватные меры - подтверждает наш предыдущий тезис о том, что кибербезопасность - это не затраты, а стоящие инвестиции.

F) Что должна делать ваша организация

Учитывая вышеизложенное, из решения Судебной палаты можно вывести определенные практические рекомендации:

Тщательно и регулярно проверяйте свою политику безопасности, чтобы убедиться, что ваши меры кибербезопасности являются (и остаются) адекватными и соразмерными риску, который обработка представляет для основных прав субъектов данных;

Если в системах еще не включено ведение журнала, проверьте, может ли оно быть полезным; там, где ведение журнала уже ведется, убедитесь, что в нем собрана вся информация, которая может быть полезна для целей доказательства, и что период хранения согласован с рисками;

В случае утечки данных или любого другого инцидента примите (незамедлительно) соответствующие меры для устранения риска и / или ограничения риска подобных инцидентов в будущем и задокументируйте их». ***(Insufficient cybersecurity measures under GDPR: 100k EUR fine in Belgium & key fines elsewhere // NautaDutilh (https://www.e-nautadutilh.com/56/4427/landing-pages/news-item.asp?sid=afca1c17-14df-44d1-a78e-615e0c7c2f74). 29.04.2021).***

***

«Компаниям необходимо обеспечить безопасность своих учетных записей пользователей. Но в дарквебе хакерам доступны миллиарды пар имен пользователей и паролей. Склонность пользователей повторно использовать пароли для нескольких учетных записей означает, что хакеры могут уже иметь учетные данные ваших пользователей, украденные у взломанной третьей стороны.

Результатом является атака с заполнением учетных данных. Заполнение учетных данных происходит, когда хакеры систематически пытаются использовать сотни или даже тысячи возможных пар имени пользователя и пароля, пока не найдут ту, которая работает.

«Каждый день вы слышите о новом миллиардах записей, которые распространяют хакеры», - комментирует Стив Томас, соучредитель и генеральный директор HackNotice. «Итак, у хакеров действительно есть ключи от королевства; они знают каждое имя пользователя и пароль, которые использовались для чего угодно, от Spotify до Gmail и всех основных сервисов - и даже банковских счетов. Проблема в том, что пользователи - большинство пользователей - по-прежнему повторно используют пароли». Следовательно, компании подвергаются риску взлома, даже если они никогда не передавали учетные данные отдельного пользователя.

Хакеры могут иметь многие тысячи имен пользователей «Джон Смит», не зная, принадлежат ли они их следующей цели. Их решение состоит в том, чтобы автоматизировать процесс тестирования каждой пары, которая у них есть, в поисках подходящей.

Существуют методы проверки того, находятся ли пароли в темной сети и, следовательно, существует ли риск их использования при заполнении учетных данных; но для этого обычно требуется предоставить данные о пользователе другой компании. Это создает загадку: безопасность требует, чтобы вы предоставляли данные пользователя службе мониторинга темной сети, в то время

как соблюдение правил конфиденциальности может потребовать, чтобы вы этого не делали.

Эту проблему решает новый сервис от HackNotice: Dark Hash Collisions (без связи или связи с организацией майнинга криптовалют, известной как DarkHash). HackNotice может сообщить компании, у кого из ее пользователей есть пароль, известный хакерам, без необходимости знать имена пользователей. Поскольку в HackNotice не передается никакая личная информация о пользователях, соблюдение требований гарантируется.

Процесс

HackNotice провел последние три года, собирая каждую пару имени пользователя и пароля, которую он мог найти в темной сети. В нем около 14 миллиардов пар. Ежегодно эта цифра увеличивается на много миллиардов по мере обнаружения новых утечек.

Для службы Dark Hash Collisions часть идентификатора пользователя на основе электронной почты удалена, оставив только чистое имя пользователя. HackNotice уже много месяцев потратил на вычислительную мощность Amazon, хешируя каждое из этих имен пользователей с помощью SHA-512. Результат - хеш и пароль. Для процесса важна только первая половина хеша.

Заказчик делает то же самое, создавая хэши SHA-512 имен пользователей в своих пользовательских базах данных. Однако он разрезает их пополам и передает HackNotice только первую половину. Это «темный хеш», поскольку он не может быть преобразован в полное имя пользователя.

Тем не менее, этой половины хеша достаточно для сопоставления с полными хешами в базе данных HackNotice. Несмотря на то, что никакие идентифицируемые личные данные не покидают клиента, у HackNotice теперь есть все необходимое, чтобы определить, какие пароли, связанные с каждым пользователем, доступны хакерам в темной сети - и, следовательно, представляют риск атак с заполнением учетных данных.

Конечно, обычные имена, такие как John Smith, могут иметь тысячи или даже миллионы разных паролей в базе данных HackNotice. HackNotice не знает, что это Джон Смит, а просто сопоставляет полученный полухеш с данными из своей базы данных - и передает их обратно заказчику.

Затем клиент может определить, есть ли у John Smith в его базе данных какие-либо взломанные пароли. Если он находит совпадение, он может либо принудительно сбросить пароль, либо потребовать от пользователя сделать это.

В начале этого процесса может быть задействовано огромное количество людей. На каждую половину хэша, которую клиент передает HackNotice, он, вероятно, получит обратно много скомпрометированных паролей. «Если клиент предоставит нам шесть миллионов полухешей, мы, вероятно, отправим обратно порядка нескольких миллиардов наборов учетных данных для проверки», - объясняет Томас. «Это будет зависеть от количества паролей, которые мы видим для каждого имени пользователя, но в среднем мы увидим от 4 до десятка паролей для очень разных имен пользователей и десятки тысяч для очень распространенных имен пользователей».

С точки зрения вычислений, однако, это простая задача для клиента - увидеть, существуют ли какие-либо скомпрометированные пары имя / пароль среди его собственных пользователей.

Если компания перейдет на службу мониторинга HackNotice, эти цифры будут быстро сокращаться. HackNotice продолжает добавлять новые утечки в свою базу данных, но будет возвращать клиенту только новые пары.

Преимущества

Важным аспектом этой услуги является то, что она может контролировать имена пользователей, подвергающихся риску, в большом масштабе, но никогда не требует от клиента раскрытия идентифицируемой личной информации третьей стороне. «Мы хотим, чтобы это была служба безопасности, которую любит команда юристов», - объясняет Томас. «Нам не отправляется ничего, что касается конфиденциальности, ничего не отправляется нам, что касается соблюдения требований. Фактически, то, что входит и уходит, - это полная чушь, но как только это снова попадает в руки клиента, у него появляется живой разум».

Этот интеллект можно использовать по-разному. Самый очевидный - защитить компанию от вброса учетных данных. Но предположим, что конкретный пользователь продолжает появляться в списке взломанных - пользователю, возможно, пришлось сбросить свой пароль, но он был быстро повторно скомпрометирован. Это может указывать на то, что пользователь плохо понимает пароль и плохо разбирается в паролях, или может указывать на то, что на компьютере пользователя есть вредоносное ПО для кражи информации.

Возможно даже, что если клиент получает большое количество совпадений из полухешей, которые он отправляет в HackNotice, это может указывать на необнаруженное нарушение со стороны клиента. Здесь Томас предостерегает от поспешных выводов. «Другая возможность состоит в том, что среди пользователей может быть высокая корреляция с другой компанией, что на самом деле было нарушено», - сказал он. Например, региональный банк может иметь большое количество пользователей, перекрестных с региональной телекоммуникационной компанией, и пользователи обычно могут повторно использовать учетные данные с обоими. Таким образом, в случае взлома региональной телекоммуникационной компании пользователи регионального банка будут особенно подвержены риску после утечки данных. Это также может произойти с другими поставщиками по всей цепочке поставок».

HackNotice также предлагает опцию запроса в реальном времени для проверок по требованию. Так, например, особенно крупные финансовые транзакции заслуживают проверки на предмет утечки учетных данных пользователя в темную сеть. Успешное обращение не означает, что пользователь является мошенником, но оно предупреждает клиента о том, что транзакция может быть совершена, и что необходимо принять дополнительные меры по борьбе с мошенничеством.

Суть в том, что Dark Hash Collisions может безопасно обнаруживать всех пользователей клиента, которые были скомпрометированы и, следовательно, представляют риск заполнения учетных данных. «По сравнению с существующей реактивной кибербезопасностью, - сказал Томас, - мы можем упреждающе

определять, когда хакеры нацеливаются на клиентов в будущем, останавливая атаки до их начала». ***(Kevin Townsend. Dark Hash Collisions: New Service Confidentially Finds Leaked Passwords // Wired Business Media (https://www.securityweek.com/dark-hash-collisions-new-service-confidentially-finds-leaked-passwords). 28.04.2021).***

***

«Австралийский разработчик программного обеспечения Click Studios в субботу призвал клиентов Passwordstate сбросить все свои пароли, если они загрузили зараженное обновление с помощью функции обновления программного обеспечения на месте.

Компания заявляет, что эта функция обслуживала зараженное обновление после того, как злоумышленник сумел скомпрометировать директор обновления на веб-сайте clickstudios.com.au. Брешь закрылась примерно через 28 часов.

«Считается, что затронуты только клиенты, которые выполнили обновления на месте в период, указанный выше. Обновление Passwordstate вручную не нарушается. Записи паролей затронутых клиентов могли быть собраны», - сообщает Click Studios.

Пострадавшие клиенты корпоративного менеджера паролей могли загрузить неправильно сформированный пакет обновления, содержащий измененный файл moserware.secretsplitter.dll, предназначенный для получения дополнительного содержимого из удаленного места и запуска вредоносного процесса.

Этот процесс собирает и эксфильтрует разнообразную системную информацию, включая имя компьютера, имена пользователей, имя и идентификатор текущего процесса, имя домена, запущенные процессы и службы, отображаемое имя и статус, адрес прокси-сервера для Passwordstate, а также имя пользователя и пароль диспетчера паролей.

Вредоносный процесс собирает из Passwordstate большой объем данных, включая URL-адреса, имена пользователей, пароли, заметки и другую информацию, хранящуюся в приложении…

Click Studios сообщает, что количество пострадавших пользователей невелико и что они связались с активными клиентами, чтобы сообщить им об инциденте». ***(Ionut Arghire. Passwordstate Users Told to Reset All Passwords Following Cyberattack // Wired Business Media (https://www.securityweek.com/passwordstate-users-told-reset-all-passwords-following-cyberattack). 26.04.2021).***

***

Кібербезпека Інтернету речей

«Согласно опросу, проведенному HSB, входящей в состав Munich Re, автомобилистов США беспокоит кибербезопасность подключенных к ним автомобилей. Некоторые даже считают, что хакер может противостоять им через

их автомобильные аудиосистемы или отключить функции автомобильной безопасности.

Подключенные автомобили и кибербезопасность

Опрос HSB, проведенный Zogby Analytics, показал, что 37 процентов ответивших потребителей были в той или иной степени или очень обеспокоены кибербезопасностью и безопасностью подключенных и автоматизированных транспортных средств.

Аналогичное число (35 процентов) опасалось, что вирус, хакерский инцидент или другая кибератака могут повредить или уничтожить данные, программное обеспечение или операционные системы их транспортных средств.

Согласно аналогичному выводу, 11 процентов ответивших заявили, что они водят электромобиль, и 50 процентов из них обеспокоены тем, что зарядные станции могут стать точкой входа для кибератаки.

Из 55 процентов потребителей, которые синхронизируют смартфоны или другие устройства, 51 процент не знают или не уверены, какая личная информация хранится в развлекательной системе их автомобиля.

«Наши автомобили связаны между собой как никогда», - сказал Тимоти Зейлман, вице-президент HSB, поставщика услуг киберстрахования. «Потребителям трудно идти в ногу с быстро развивающимися автомобильными технологиями, и они задаются вопросом, защищена ли их конфиденциальность и личная информация».

Водители обеспокоены удаленным управлением автомобилями

Каждый десятый потребитель сообщил о взломе или другой кибератаке, затронувшей его автомобиль, что на три процента больше, чем в аналогичном опросе HSB годом ранее.

Поскольку сетевые технологии продолжают развиваться, некоторые обеспокоены не только тем, что их автомобиль может быть взломан, но и тем, что другие могут управлять удаленно.

На вопрос, что их больше всего беспокоит в связи с возможной кибератакой на их автомобиль, 46 процентов потребителей были очень обеспокоены тем, что хакер может связаться с ними через их аудиосистему, возможно, чтобы принудить их или потребовать выкуп.

Другими наиболее серьезными проблемами были обездвиженность их автомобиля (25 процентов очень обеспокоены), скомпрометированные системы безопасности (23 процента) и блокировка их транспортного средства (14 процентов).

Наиболее распространенные технологии, устанавливаемые в транспортных средствах, включают Bluetooth (53 процента), навигационные системы (42 процента) и датчики безопасности транспортных средств (39 процентов).

Тридцать шесть процентов потребителей владеют приложениями для смартфонов, которые подключаются к их транспортным средствам, в то время как 24 процента имеют Wi-Fi или мобильные точки доступа, которые предоставляют интернет-услуги в дороге». ***(Consumers worry about the cybersecurity of connected vehicles // Help Net Security***

(https://www.helpnetsecurity.com/2021/04/16/cybersecurity-connected-vehicles/). 16.04.2021).

***

«**Девять уязвимостей, обнаруженных Forescout Research Labs и JSOF Research, значительно увеличивают поверхность атаки как минимум 100 миллионов устройств Интернета вещей, подвергая их потенциальным атакам, которые могут вывести устройства из строя или быть захваченными злоумышленниками.**

«История показала, что управление устройствами Интернета вещей может быть эффективной тактикой для запуска DDoS-атак», - сказал Рохит Даманкар, вице-президент по продуктам анализа угроз компании Alert Logic, занимающейся безопасностью приложений и инфраструктуры в Хьюстоне.

«По мере того, как устройства IoT становятся богаче функциональными, они могут оказаться под контролем злоумышленника, как серверы или настольные компьютеры, и в дальнейшем могут быть использованы в качестве плацдарма для взломов предприятий», - сказал он TechNewsWorld.

Названный Name: Wreck, набор уязвимостей затрагивает четыре популярных стека TCP / IP - FreeBSD, Nucleus NET, IPnet и NetX.

Исследователи объяснили в блоге, что Nucleus NET является частью Nucleus RTOS, операционной системы реального времени, используемой более чем тремя миллиардами устройств, включая ультразвуковые аппараты, системы хранения данных, критически важные системы для авионики и другие.

Исследователи отметили, что FreeBSD широко используется высокопроизводительными серверами в миллионах ИТ-сетей, а также является основой для других хорошо известных проектов с открытым исходным кодом, таких как межсетевые экраны и несколько коммерческих сетевых устройств.

Они добавили, что NetX обычно работает под управлением ОСРВ ThreadX, которая в 2017 году развернулась 6,2 миллиарда и может использоваться в медицинских устройствах, системах на кристалле и нескольких моделях принтеров.

«Организации в сфере здравоохранения и государственного сектора входят в тройку наиболее пострадавших по всем трем стекам», - пишут исследователи. «Если мы консервативно предположим, что один процент из более чем 10 миллиардов развертываний, описанных выше, уязвим, мы можем оценить, что по крайней мере 100 миллионов устройств затронуты Name: Wreck».

Мощный вектор атаки

Эксперты по безопасности сообщили TechNewsWorld, что атаки TCP / IP могут быть особенно мощными.

«TCP / IP - это программное обеспечение, которое на самом деле осуществляет всю связь от устройства к другим системам», - пояснил Гэри Кингхорн, директор по маркетингу Tempered Networks, компании по микросегментации в Сиэтле.

«Если это сетевая атака - в отличие от вставки флэш-накопителя в USB-порт - вы должны использовать TCP / IP», - сказал он. «Повреждение программного

обеспечения TCP / IP для обнаружения уязвимостей или использование ошибок в конструкции - основа большинства атак».

Атаки на стек TCP / IP также могут обойти некоторые элементарные меры безопасности.

«Каждый раз, когда у вас есть атака на TCP / IP, и вам не нужно имя пользователя или пароль, выполнить атаку проще», - заметил Дхаманкар.

«Уязвимости TCP / IP являются мощными, поскольку их можно использовать удаленно через Интернет или в интрасети без необходимости подрывать другие механизмы безопасности, такие как аутентификация», - добавил Боб Баксли, технический директор Bastille Networks из Сан-Франциско, поставщика средств обнаружения угроз и безопасность для Интернета вещей.

Кроме того, после взлома устройства злоумышленник может получить бонус для атакующего TCP / IP. «В большинстве случаев код стеков TCP / IP работает с высокими привилегиями, поэтому любая уязвимость выполнения кода позволит злоумышленнику получить значительные привилегии на устройстве», - сказал Асаф Карас, соучредитель и технический директор Vdoo, поставщика средств автоматизации безопасности. для встраиваемых устройств в Тель-Авиве, Израиль.

Проблемы с исправлением

Хотя некоторые из уязвимостей, выявленных исследователями, можно исправить, этот процесс может быть проблематичным.

Баксли отметил, что были выпущены исправления для FreeBSD, Nucleus NET и NetX.

«Для конечных устройств, использующих эти стеки, теоретически возможно исправление», - сказал он. «Но на практике многие уязвимые системы представляют собой устройства IoT, работающие под управлением операционных систем реального времени, которые не входят в обычный график исправлений и вряд ли получат исправления».

«Устройства Интернета вещей обычно обрабатываются по принципу« развернуть и забыть »и часто заменяются только после того, как они выйдут из строя или достигли конца срока службы», - добавил Жан-Филипп Таггарт, старший исследователь безопасности в Malwarebytes.

«Это не очень эффективный подход», - сказал он TechNewsWorld.

Возраст может быть еще одной проблемой для устройств Интернета вещей. «Эти системы могут быть исправлены, но, как правило, это очень старые реализации, которые можно использовать для сценариев, для которых они не были предусмотрены», - заметил Кингхорн.

«Они уязвимы из-за своей абсолютной сложности и неспособности легко идентифицировать риски», - продолжил он. «Чаще всего хакеры могут использовать их до того, как они будут исправлены».

«Всегда было очень сложно исправить уязвимости Интернета вещей», - добавил Дхаманкар. «Достаточно сложно исправить уязвимости серверов и настольных компьютеров».

Тактика защиты

Даже без патчей есть способы защитить сеть от эксплуататоров уязвимостей, обнаруженных исследователями Forescout и JSOF.

Бэксли объяснил, что для использования уязвимостей Name: Wreck злоумышленник должен ответить на запрос DNS от целевого устройства поддельным пакетом, содержащим вредоносную полезную нагрузку. Для этого злоумышленнику потребуется сетевой доступ к целевому устройству.

«Хранение устройств, особенно устройств IoT, сегментированных от Интернета и основных внутренних сетей, является одним из механизмов снижения риска заражения», - сказал он.

Мониторинг DNS также может помочь защититься от Name: Wreck. «Мониторинг активности DNS в среде и отметка любой активности внешнего DNS-сервера - хороший шаг», - заметил Дхаманкар.

«В целом, - добавил он, - DNS - отличный источник для отслеживания компромиссов с помощью аналитики безопасности».

Улучшенное управление доступом также может помешать злоумышленникам. «Если сама система не может быть исправлена, и это может иметь место в случае устаревших промышленных систем управления или других сетевых устройств OT и конечных точек IoT, важно убедиться, что сеть разрешает только безопасный, доверенный трафик на эти устройства», - сказал Кингхорн. объяснил.

«Здесь могут помочь проекты Zero Trust, гарантирующие, что только авторизованные устройства могут получить доступ к этим уязвимым системам», - продолжил он. «Это также может помочь в постоянном мониторинге и анализе трафика на эти устройства, чтобы гарантировать, что потенциально вредоносный или подозрительный трафик не достигает их».

«Интернет вещей в целом является горячей точкой для обеспечения безопасности», - добавил Крис Моралес, директор по информационной безопасности компании Netenrich, поставщика услуг центра безопасности в Сан-Хосе, Калифорния.

«Слабые пароли и жестко запрограммированные учетные записи пользователей, отсутствие исправлений и устаревших компонентов - эти последние уязвимости - это всего лишь еще одна проблема, связанная с небезопасным Интернетом вещей», - сказал он TechNewsWorld». ***(John P. Mello Jr. DNS Flaws Expose Millions of IoT Devices to Hacker Threats // TechNewsWorld (https://www.technewsworld.com/story/87096.html). 14.04.2021).***

***

«Поскольку пандемия продолжает способствовать переходу к удаленной работе, многочисленные производители воспользовались этим движением, чтобы создать множество удобных устройств Интернета вещей (IoT). Хотя эти устройства могут сделать наш дом и работу более удобными, они значительно расширяют поверхность атаки для киберпреступников. Здесь мы рассмотрим лучшие методы кибербезопасности, которые могут предотвратить атаки.

Устройства Интернета вещей создают множество уязвимостей в сетях организаций, и их часто сложно исправить. По оценкам, к 2025 году количество активных подключений устройств Интернета вещей превысит 30 миллиардов, и специалистам по информационной безопасности необходимо найти эффективную

платформу для более эффективного мониторинга и защиты устройств Интернета вещей от использования для распределенного отказа или обслуживания (DDoS), программ-вымогателей или даже кражи данных.

Когда удобство камеры дверного звонка, робота-пылесоса или термостата, активируемого мобильным телефоном, может потенциально нанести финансовый ущерб или угрожать физическому ущербу, к безопасности этих устройств нельзя относиться легкомысленно. Мы должны переориентировать наше мышление в отношении кибергигиены, чтобы рассматривать эти устройства как потенциальные угрозы для наших конфиденциальных данных. Существует слишком много примеров, когда злоумышленники получают доступ к предположительно незначительному устройству IoT, например, системе управления HVAC для глобальной розничной сети, только для того, чтобы переключиться на другие незащищенные устройства в той же сети, прежде чем получить ценную конфиденциальную информацию.

Хотя фишинг остается наиболее популярным вектором атак, что усиливает потребность людей быть неотъемлемой частью надежной программы безопасности, устройства Интернета вещей теперь предлагают киберпреступникам еще один способ доступа к учетным записям и сетям для кражи данных, проведения разведки и дальнейшего развертывания вредоносных программ. Недавние случаи показали примеры этого:

В 2019 году киберпреступники смогли получить доступ к базе данных казино о «высоких игроках», взломав умный термометр в аквариуме в вестибюле казино, а затем подключившись к сети казино;

Уязвимости в домашней системе сигнализации привели к тому, что киберпреступники провели DDoS-атаку, используя эти устройства в ботнете в качестве механизма распространения вредоносного ПО;

А внешний динамик, подключенный к Bluetooth, позволял хакерам подслушивать его конфиденциальные разговоры, пока он работал из дома.

Когда мы думаем об использовании устройств IoT сегодня, последствия их взлома могут нанести значительный ущерб. Например, успешная компрометация термостата, подключенного к Интернету, может поставить под угрозу целостность чувствительных помещений с контролируемым климатом, в которых хранятся фармацевтические препараты (включая вакцины), продукты питания и другие скоропортящиеся товары.

Ключевые элементы управления безопасностью для устройств Интернета вещей

Производственный цикл проектирования устройств IoT редко включает реализацию безопасности в процессе разработки. Такой надзор привел к увеличению количества успешных компромиссов, и не обязательно в результате изощренных атак. Некоторые из основных методов компрометации Интернета вещей и мер безопасности для устранения этих уязвимостей включают:

1. Пароли по умолчанию

Как и большинство новых устройств, которые подключаются к сети, многие машины Интернета вещей предоставляют пароли по умолчанию. К сожалению, при большом количестве украденных IP-адресов, доступных на рынках даркнета, если

пользователь по-прежнему использует пароль по умолчанию (также доступный в темной сети) или простой пароль, который подвержен атакам грубой силы, это может быть легко способ для злоумышленников получить дальнейший доступ к сети и, возможно, к конфиденциальным данным, хранящимся в этой сети.

2. Непропатченные функции безопасности

Неустановленное оборудование и программное обеспечение уже много лет являются основной целью киберугроз. Недавно мы увидели, как неустановленные операционные системы привели к глобальной атаке программы-вымогателя WannaCry на компьютеры Windows; эксплуатируются незащищенные уязвимости программной платформы, например, те, с которыми сталкиваются пользователи Citrix; и даже в 2020 году незащищенные эксплойты Eternal Blue использовались злоумышленниками для развертывания крупномасштабных атак программ-вымогателей на скомпрометированные сети.

Подобные атаки на незащищенные уязвимости позволяют киберпреступникам перемещаться вбок после того, как они закрепятся в сети. Это оказалось крайне катастрофическим для большого количества жертв атак банковских троянов и программ-вымогателей. Политика управления исправлениями должна быть создана для автоматизации исправлений, когда они предоставляются производителями оборудования и программного обеспечения, а также для предоставления рекомендаций по немедленной установке исправлений, необходимых для критических систем.

3. Плоские сети

Успех атак IoT обычно достигается, когда скомпрометированное устройство IoT подключено к сети, которая содержит конфиденциальные или важные данные. Устройства Интернета вещей должны быть отделены от других систем в сети, чтобы ограничить способность злоумышленника перемещаться вбок туда, где они могут нанести наибольший ущерб, как финансовый, так и инфраструктурный.

4. Сетевая инвентаризация

ИТ-команды должны периодически проводить инвентаризацию своих сетей, чтобы определять, какие устройства подключены, и проверять, были ли они одобрены. Это также позволит командам исправлять эти устройства теперь, когда они знают, что они активны в сети. Мы видели слишком много ситуаций, когда злоумышленники имели доступ к сети в течение месяцев (и более), когда существовала неуверенность в отношении доступа к сети неавторизованных устройств или учетных записей. Эта безрезультатная ситуация дает злоумышленникам неограниченный доступ для незаметного проведения разведки и выявления не только важных данных, имеющих денежную ценность, но также для изучения конфигураций и функций безопасности и развертывания дополнительных вредоносных программ.

5. Bluetooth

Многие устройства Интернета вещей используют Bluetooth в качестве метода подключения к сети. Однако в Bluetooth есть уязвимости в системе безопасности, которые могут сделать эти устройства открытыми для атак. Это особенно важно, если подумать о потенциальном воздействии на медицинские устройства и имплантаты с поддержкой Bluetooth, когда компрометация может привести к краже

PII / PHI или поставить под угрозу здоровье пациента, если устройство будет отключено. Настоятельно рекомендуется, чтобы пользователи устанавливали режим без возможности обнаружения при использовании устройств IoT, сопряженных с Bluetooth. По мере того, как хакеры продолжают выявлять уязвимости Bluetooth, важно исправлять прошивку для устройств с поддержкой Bluetooth, поскольку эти меры безопасности предоставляются производителями.

По мере того, как мы приближаемся к середине 2021 года, существует общее понимание (и потребительский спрос), что будет доступно больше устройств IoT для оказания множества услуг. Эти устройства используются во многих отраслях промышленности и варьируются от домашнего и потребительского использования до коммерческих приложений. Хотя они предлагают множество ценных функций и удобств, они также создают потенциальный риск компрометации конфиденциальных данных или несанкционированного доступа к личным, корпоративным и государственным сетям. Идентификация и защита вашей сети устройств IoT сегодня может сэкономить ваше время, данные и капитал в будущем. Но будьте осторожны - это не разовое мероприятие, и по мере изменения технологий должны меняться и ваши средства управления». ***(Matt Dunn. 5 Fundamental But Effective IoT Device Security Controls // Threatpost (https://threatpost.com/5-fundamental-iot-device-security-controls/165577/). 23.04.2021).***

***

Кіберзлочинність та кібертероризм

«Предполагается, что злоумышленники нацелены на школьные округа в округе Сомерсет, штат Нью-Джерси.

Инциденты безопасности, произошедшие в округе за последнюю неделю, привели к закрытию школ в двух учебных заведениях на целый день. Школы в Бернарде были закрыты 7 апреля, а школы Хиллсборо были закрыты 12 апреля из-за подозрений в кибератаках.

Компьютерные системы и голосовая почта персонала в Хиллсборо во вторник остались неработоспособными. Тем не менее, студенты и сотрудники получили виртуальный доступ к урокам.

«Наша технологическая команда продолжает методично работать с экспертами по кибербезопасности и правоохранительными органами, чтобы установить график завершения восстановления работы наших систем», - сообщила родителям директор школ Хиллсборо Лиза Антунес в электронном письме от 13 апреля.

Она добавила: «Это чрезвычайно сложная задача с множеством движущихся частей».

Пока расследование инцидента продолжается, суперинтендант не хотел раскрывать многие детали.

«Мы очень ограничены в том, чтобы делиться множеством факторов, влияющих на информацию, которую мы можем предоставить сотрудникам и

семьям», - сказал Антунес. «График завершения восстановления работы наших систем не может быть предоставлен в настоящее время».

Она добавила, что решение о закрытии школы в понедельник было принято по совету ФБР и правоохранительных органов «с целью минимизировать ущерб организации», что открывает возможность того, что район был поражен программой-вымогателем.

«Несколько часов назад наш технологический отдел был предупрежден о возможной кибератаке», - написал Антунес в сообщении, размещенном на школьной странице Messenger.

«Правоохранительные органы, в том числе ФБР, рекомендовали отключить наши системы, чтобы мы могли определить глубину атаки».

Директор школ Bernards Ник Маркарян сказал родителям, что инцидент, связанный с безопасностью округа, был «сфокусирован на сервере». Он сказал, что отдельные устройства Chromebook, ноутбуки, смартфоны и другие устройства, подключенные к районной сети, не были взломаны.

Маркарян добавил, что «в ближайшие дни ко всем устройствам, выпущенным в округе, будут добавлены дополнительные средства защиты, чтобы по-новому контролировать их здоровье» в качестве меры предосторожности». ***(Sarah Coble. New Jersey School Districts Investigate Cyber-Attacks // Reed Exhibitions Ltd (https://www.infosecurity-magazine.com/news/new-jersey-schools-cyber-attack/). 14.04.2021).***

***

«Университет Хартфордшира в Великобритании подвергся кибератаке, в результате которой была отключена вся его ИТ-сеть, а также заблокирован доступ к его облачным сервисам.

Высшее учебное заведение сообщило, что атака произошла поздно вечером в среду 14 апреля, в заявлении, размещенном на его веб-сайте ранее сегодня. В результате все его онлайн-занятия, запланированные сегодня (15 апреля), были отменены.

В заявлении говорилось: «Незадолго до 22:00 прошлой ночью в университете произошла кибератака, которая затронула все наши системы, в том числе облачные, такие как Canvas, MS Teams и Zoom. Будьте уверены, наши ИТ-коллеги прилагают все усилия, чтобы исправить ситуацию как можно скорее.

«Однако в результате все онлайн-обучение будет отменено сегодня (четверг, 15 апреля), и мы понимаем, что это может повлиять на возможность учащихся сдавать задания. Мы хотим заверить наших студентов в том, что из-за этого никто не окажется в невыгодном положении.

«Любое личное обучение в кампусе может продолжаться и сегодня, если доступ к компьютеру не требуется, но у студентов не будет локального или удаленного доступа к компьютерным средствам в LRC, лабораториях или университетскому Wi-Fi.

«Приносим извинения за неудобства, которые возникли в результате этой ситуации, и будем держать вас в курсе. Вы можете проверить статус всех наших систем, посетив https://status.herts.ac.uk/.

В настоящее время нет более подробной информации о характере атаки, хотя в прошлом году произошло резкое увеличение числа атак программ-вымогателей, нацеленных на высшие учебные заведения, отчасти из-за дополнительных уязвимостей, вызванных переходом на онлайн-обучение во время COVID. -19. В прошлом году в университетах Великобритании Ньюкасл и Нортумбрия произошли инциденты с программами-вымогателями, что привело к серьезным сбоям в работе.

Комментируя это, Жером Робер, директор Alsid, объяснил, что существует ряд причин, по которым университеты создают соблазнительные мишени для киберпреступников.

«Университеты все больше осознают, что они являются основными целями кибератак и программ-вымогателей. Хотя карманы университетов не так велики, как у крупных предприятий, существует множество характеристик, которые делают их уязвимыми для атак такого рода», - сказал он.

«Огромный размер студентов и преподавателей в университете - в случае Хартфордшира почти 28 000 человек - делает невероятно сложным обеспечение безопасности ИТ-инфраструктуры и управление ею. Подумайте об огромном количестве новых участников и выпускников каждый год в университетах: ИТ-команды каким-то образом должны управлять процессом создания, удаления и управления всеми этими учетными записями. Это бесконечная операция по поддержанию всего этого в чистоте и порядке, и любые упущения, такие как не закрытие старых счетов, представляют собой риск. Вдобавок к этому высшее образование в настоящее время подвергается повышенному риску из-за увеличения сетевой активности и общей сложности обеспечения гибридного обучения». ***(James Coker. Uni of Hertfordshire Suffers Cyber-Attack That Takes Down its Entire IT Network // Reed Exhibitions Ltd (https://www.infosecurity-magazine.com/news/uni-hertfordshire-cyber-attack-it/). 15.04.2021).***

***

«Кибератакам подвергаются не только корпорации, государственные учреждения и технологические компании. Школьные округа также входят в список жертв киберпреступников, и Austin ISD стала одной из последних жертв взлома, вызванного сторонним удаленным доступом.

Компания Austin ISD обнаружила утечку данных после того, как узнала о письме от предыдущего стороннего поставщика, PCS Revenue Control Systems, Inc., которое было отправлено семьям относительно взлома. В письме сообщалось, что имя указанного студента, его идентификационный номер и дата рождения потенциально подверглись несанкционированному доступу во время утечки данных в декабре 2019 года. Тем, кто пострадал, предлагается бесплатный мониторинг личности в результате атаки.

Этот пример является лишь одним из многих примеров в сфере образования: в сентябре 2015 года университет Рутгерса стал жертвой DDoS-атаки, а в марте 2018 года школьный округ округа Леон потерял личную информацию примерно 50 000 студентов и сотрудников из-за сторонний поставщик, Виртуальная школа Флориды (FLVS). Информация, предоставленная об учениках, включала имя, имя

пользователя, школьный идентификационный номер, медицинские и демографические данные. Раскрытая конфиденциальная информация сотрудника включала номера социального страхования, полную контактную информацию, адреса электронной почты и многое другое.

Помимо нарушения правил школьного округа округа Леон, FLVS потеряла данные школьного округа в двух других отдельных инцидентах, включая следующие:

В 2013 году школьный округ округа Леон предоставил поставщику электронных услуг, UCompass, доступ к данным о персонале округа и учащихся. Позднее FLVS приобрела UCompass и получила данные, сохранив их на небезопасном сервере. В феврале 2018 года неавторизованный злоумышленник получил доступ к незащищенному серверу и опубликовал свои выводы на онлайн-форуме. Школу предупредил сотрудник Databreaches.net, который заметил комментарий на форуме.

С мая 2016 года по февраль 2018 года FLVS предоставляла образовательные онлайн-услуги пользователям во всем школьном округе округа Леон. В феврале 2018 года FLVS уведомил школьный округ о том, что личные данные, переданные за это время, стали общедоступными.

Важность кибербезопасности в школах

Хотя не было никаких доказательств того, что нарушение Остина ISD использовалось в злонамеренных целях, этот сценарий является еще одним примером ущерба и ответственности, которые возникают, когда сторонний поставщик не имеет надежной или даже адекватной сетевой безопасности. Если хакер действительно имел злонамеренный умысел, ущерб мог бы распространиться на крупные выплаты выкупа или огромные потери репутации: восемьдесят семь процентов потребителей готовы уйти и заняться своим бизнесом в другом месте, если или когда произойдет утечка данных. Для сторонних поставщиков, обслуживающих системы образования, это должно стать тревожным сигналом. Доверие и репутация надежного делового партнера находятся под угрозой, когда подключение не защищено или не контролируется.

Для школьных округов любая угроза нападения - лично или через Интернет - должна быть устранена и защищена. Это правильный протокол. Защита ваших сотрудников и вашей компании включает в себя защиту их от кражи и раскрытия конфиденциальной и важной информации, которую можно найти только во внутренних системах. Управление сторонним удаленным доступом и реализация сторонней программы управления рисками - это первые шаги к защите сетей школьного округа от хакеров, использующих сторонние точки доступа.

Для поставщиков образовательных систем упреждающий подход к сетевой безопасности является основой качественного поставщика услуг. Платформы удаленной поддержки не только служат дополнительным преимуществом, но и усиливают защитные меры, которые ваша компания примет для обеспечения безопасности вашего клиента - в данном случае защита PII студентов и сотрудников». ***(Tori Taylor. A lesson in cybersecurity for school districts // Security Boulevard (https://securityboulevard.com/2021/04/a-lesson-in-cybersecurity-for-school-districts/). 09.04.2021).***

***

«Еще один пример устойчивости и креативности кибер-злоумышленников изложен в новом блоге исследователей Cisco / Talos, в котором рассказывается, как за последний год и, в частности, в результате миграции с работы в офисе на работу из дома во время пандемии кибер-злоумышленники используют платформы для совместной работы, такие как Slack и Discord, для распространения вредоносных программ среди ничего не подозревающих жертв.

Согласно блогу:

Поскольку удаленная работа стала нормой на протяжении всей пандемии COVID-19, злоумышленники меняют свою тактику, чтобы воспользоваться изменениями в рабочих процессах сотрудников.

Злоумышленники используют платформы для совместной работы, такие как Discord и Slack, чтобы оставаться незамеченными и уклоняться от защиты организации.

Платформы для совместной работы позволяют злоумышленникам проводить кампании с использованием законной инфраструктуры, которая не может быть заблокирована во многих сетевых средах.

Трояны удаленного доступа (RAT), кражи информации, вредоносные программы для Интернета вещей и другие угрозы используют платформы для совместной работы для доставки, извлечения компонентов и обмена данными для управления и контроля.

В общем, комнаты и платформы для совместной работы используются для «распространения традиционных приманок вредоносного спама, используемых для заражения жертв». Они используют платформы, чтобы «обойти меры безопасности по периметру и максимально увеличить возможности заражения». Они используются на трех этапах атак вредоносного ПО, включая доставку, извлечение компонентов, а также C2 и кражу данных. Они также используются в кампаниях социальной инженерии.

Если ваша организация использует платформы для совместной работы, важно, чтобы ваши ИТ-специалисты и сотрудники знали о злонамеренном использовании этих платформ, чтобы они могли использовать надлежащую кибергигиеницу, чтобы избежать инцидента, как при фишинге или схеме социальной инженерии. С этими платформами для совместной работы следует использовать те же инструменты, которые они используют для выявления вредоносных электронных писем или текстов. Обучение этим схемам и использованию законных бизнес-платформ - первая защита от инцидента». ***(Linn Foster Freedman. Cisco/Talos Researchers Find Attackers Using Slack and Discord to Distribute Malware // Robinson & Cole LLP (https://www.dataprivacyandsecurityinsider.com/2021/04/cisco-talos-researchers-find-attackers-using-slack-and-discord-to-distribute-malware/). 15.04.2021).***

***

«Applus Technologies, Inc., поставщик автотранспортных средств нескольких департаментов штата, который помогает штатам в проведении инспекций транспортных средств, недавно объявил, что его системы были затронуты вредоносным ПО, что нарушило проверки транспортных средств в Коннектикуте, Джорджии, Айдахо, Иллинойсе, Массачусетсе, Нью-Йорке., Техас и Юта. Из-за отключения не удалось завершить техосмотр автомобилей с 30 марта 2021 года.

Это, очевидно, очень неудобно для тех людей, чьи контрольные наклейки имеют или скоро истекают, поскольку они рискуют получить ссылку на просроченную контрольную наклейку, помимо того, что им придется взять время, чтобы взять свою машину для осмотра.

Чтобы решить эту проблему, в Реестре автотранспортных средств штата Массачусетс (RMV) заявили: «[R] Признавая неудобства, которые вызывает отключение Applus, RMV связывался с правоохранительными органами с просьбой о сотрудничестве и осмотрительности при цитировании тех, у кого срок действия наклейки истек. кто, возможно, пытался посетить станцию на этой неделе». RMV продлил льготный период в один месяц для водителей, которые не смогли получить свои контрольные наклейки из-за сбоя в работе.

После того, как проверки были отложены на неделю, 7 апреля 2021 года Applus отправила исправление программного обеспечения на станции технического обслуживания, чтобы попытаться решить проблему. Однако сообщается, что Апплюс разослал патч на СТО на флешках! Флэш-накопители известны тем, что используются для внедрения вредоносных вредоносных программ и программ-вымогателей в системы пользователей. Отправка патча на флешку полностью противоречит лучшим практикам безопасности.

Applus заявила, что не считает, что какая-либо финансовая информация клиента (например, станции обслуживания) была скомпрометирована, но работает с экспертом-криминалистом…». ***(Linn Foster Freedman. Vehicle Inspections in Multiple States Disrupted by Malware // Robinson & Cole LLP (https://www.dataprivacyandsecurityinsider.com/2021/04/vehicle-inspections-in-multiple-states-disrupted-by-malware/). 08.04.2021).***

***

«Университет Хартфордшира пострадал от разрушительной кибератаки, в результате которой были выведены из строя все его ИТ-системы, включая Office 365, Teams и Zoom, локальные сети, Wi-Fi, электронную почту, хранилище данных и VPN.

Университет сообщил о нападении злоумышленников в среду, в результате чего были отменены все онлайн-занятия в четверг и пятницу.

«Незадолго до 22:00 в среду, 14 апреля, университет подвергся кибератаке, которая затронула все наши системы, в том числе облачные, такие как Canvas, MS Teams и Zoom», - говорится в сообщении на своем веб-сайте.

Из-за пандемических ограничений на очные занятия университет и большинство студентов по-прежнему зависят от приложений для онлайн-обучения и видеоконференций, таких как Zoom. Правительство Великобритании разрешило

некоторым студентам вернуться к очному обучению, если им требуется специальное оборудование, но запретило полное возвращение как минимум до 17 мая.

В университете отметили, что отключение питания может повлиять на отправку заданий студентами, но заверили их, что в результате ни один студент не окажется в невыгодном положении.

Студентам разрешалось посещать университет при условии, что доступ к компьютеру не был необходим.

«Вы не сможете получить доступ к компьютерному оборудованию в LRC, лабораториях или университетском Wi-Fi. Удаленный доступ к специализированному программному обеспечению и компьютерам в настоящее время недоступен», - заявили в университете.

На странице состояния системы в Хартфордшире, последний раз обновлявшейся 17 часов назад, показаны масштабы нарушения.

Неясно, какую кибератаку пережил университет, но Национальный центр кибербезопасности (NCSC) в прошлом месяце предупредил о всплеске атак программ-вымогателей на школы, колледжи и университеты.

«В недавних инцидентах, затрагивающих сектор образования, программы-вымогатели привели к потере студентами курсовых работ, финансовых отчетов школ, а также данных, относящихся к тестированию на COVID-19», - говорится в сообщении агентства». ***(Liam Tung. Cyberattack on UK university knocks out online learning, Teams and Zoom // ZDNet (https://www.zdnet.com/article/cyberattack-on-uk-university-knocks-out-online-learning-teams-and-zoom/). 16.04.2021).***

***

«Фишинговые атаки остаются огромной проблемой, и злоумышленники тратят много времени и усилий на то, чтобы для потенциальной жертвы щелчок по плохой ссылке был самым интуитивно понятным и простым делом.

Распространенный метод, используемый в электронных письмах, отправляемых киберпреступниками при попытке фишинговых атак, - это утверждение, что жертве необходимо в срочном порядке щелкнуть ссылку или загрузить вложение.

Это может быть что угодно: от важных корпоративных документов в корпоративной среде до уведомления о доставке посылки, выигрыша приза или даже фальшивой угрозы о вызове в суд.

Сообщения составлены таким образом, что щелкнуть фишинговую ссылку - это самый простой способ сделать это, чтобы направить пользователя на страницу, предназначенную для кражи учетных данных для входа или другой личной информации.

Мошенники создадут эти фишинговые страницы так, чтобы они выглядели почти неотличимыми от реальной, которую они имитируют, что является частью плана, направленного на то, чтобы сделать операцию как можно более гладкой - без причины для пользователя сомневаться в том, что что-то не так.

«Отчасти проблема заключается в том, что фишинговые сигналы часто неотличимы от положительных характеристик пользовательского опыта», - сказал ZDNet Security Update Трой Хант, создатель HaveIBeenPwned и цифровой советник Nord Security.

«Это легко, когда у вас есть ссылка, потому что вы просто нажимаете на нее, и вы попадаете прямо в нужное место, и она глубоко связывает вас с потенциально мошеннической транзакцией», - добавил он.

Например, если у пользователя возникли опасения, что ссылка, якобы принадлежащая их банку, может быть фишинговым письмом, он может не переходить по ссылке, а вместо этого открыть новое окно и перейти на веб-сайт банка, чтобы проверить, есть ли там действительно было сообщение от их аккаунта.

Таким образом они избегают потенциально опасной фишинг-ссылки. Но фишинговые атаки остаются успешными, потому что людей по-прежнему заставляют переходить по ссылкам.

И это несмотря на недавний опрос о конфиденциальности, проведенный NordVPN, который предполагает, что, хотя люди говорят, что знают, как оставаться в безопасности в Интернете, они все равно станут жертвами фишинга и других кибератак, потому что киберпреступники очень способны использовать социальную инженерию для принуждения жертв к действиям. что они хотят.

«Люди в конечном итоге подвержены ошибкам. К сожалению, это органическое вещество за клавиатурой, которое часто является уязвимой частью цикла», - сказал Хант.

«Нам необходим баланс образования и обучения, а также технологии, которые будут поддерживать это и помогать нам, когда что-то идет не так», - добавил он.

Организации могут предложить персоналу обучение, чтобы помочь им выявлять фишинговые атаки, а поощрение использования таких инструментов, как многофакторная аутентификация и менеджеры паролей, также может помочь защитить людей от фишинговых атак». ***(Danny Palmer. Why do phishing attacks work? Blame the humans, not the technology // ZDNet (https://www.zdnet.com/article/why-do-phishing-attacks-work-blame-the-humans-not-the-technology/). 08.04.2021).***

***

«Facebook удалил ферму троллей, распространителей дезинформации и создателей дипфейков в своих последних усилиях по модерации.

В последнем отчете компании о скоординированном недостоверном поведении (CIB), опубликованном на этой неделе (.PDF), перечислены последние усилия Facebook по сокращению скоординированного недостоверного поведения в сети.

Согласно мартовскому отчету CIB, Facebook расследовал и уничтожил "давнюю" ферму троллей, расположенную в Албании.

Члены «фермы троллей» в первую очередь нацелены на иранскую аудиторию и, как считается, имеют связи с «Моджахедин-э Халк» (МЕК), политико-боевой группировкой, состоящей из нескольких тысяч членов.

МЕК был сослан в Албанию и теперь, похоже, управляет сетью, состоящей как из подлинных, так и из поддельных учетных записей, для распространения информации, критикующей правительство Ирана и восхваляющей деятельность МЕК.

Facebook сообщает, что обмен контентом, связанным с МЕК, резко увеличился в 2017 и 2020 годах за счет трех отдельных кластеров, но большая часть усилий группы по увеличению аудитории потерпела неудачу.

«Большинство ее учетных записей принадлежало операторам в Албании, которые обычно совместно использовали техническую инфраструктуру», - отмечает компания. «Это означало, что один и тот же оператор мог запускать несколько учетных записей; и наоборот, несколько операторов могли запускать одну и ту же учетную запись. Это некоторые из отличительных черт так называемой фермы троллей - физического места, где коллектив операторов разделяет компьютеры и телефоны для совместного управления пулом поддельных учетных записей в рамках операции влияния».

Кроме того, Facebook борется с дипфейками, изображениями, созданными с помощью искусственного интеллекта (ИИ). Хотя компания начала снимать поддельные изображения три года назад, теперь генерирующие состязательные сети (GAN) используют дипфейки, чтобы выдать себя за независимые новостные агентства и журналистов-расследователей.

Изучив исследование, предоставленное FireEye в сети GAN, расположенной в Испании и Сальвадоре, фирма удалила аккаунты и страницы, на которых публиковалась информация о выборах мэра со скоростью, подобной "спаму". Еще две сети также были уничтожены, в результате чего общее количество удалений Facebook достигло семи операций, в которых использовались изображения, созданные искусственным интеллектом.

Гигант социальных сетей также задокументировал свое обычное нарушение работы недостоверных сетей. В общей сложности в марте были прерваны 14 операций CIB из таких стран, как Аргентина, Египет, Израиль, Мексика и Грузия, что привело к удалению более 1100 учетных записей, 255 страниц и 34 групп.

В прошлом месяце Facebook заявил, что ему удалось обнаружить и уничтожить китайскую сеть кибератак, использующих эту платформу для распространения вредоносного ПО. Операторы, которые, как считается, являются частью групп Earth Empusa или Evil Eye, использовали поддельные профили для нацеливания на журналистов и активистов.

Обновление 9/5 9.00 BST: МЕК и Национальный совет сопротивления Ирана (NCRI) отрицали существование фермы троллей и отклонили заявления Facebook об удалении учетной записи.

«МЕК никогда не использовала вымышленные личности и не использовала чужие личности», - заявляет группа. «Тем не менее, любой, особенно иранцы, выступающие против режима, имеет право использовать псевдонимы или знаки и символы, которые они предпочитают из соображений безопасности». ***(Charlie***

Osborne. Facebook tackles deepfake spread and troll farms in latest moderation push // ZDNet (https://www.zdnet.com/article/facebook-tackles-deepfake-spread-and-troll-farms-in-latest-moderator-report/). 08.04.2021).

***

«Microsoft предупреждает компании, чтобы они остерегались киберпреступников, используя контактные формы на веб - сайтах компании, чтобы доставить сотрудникам банковского трояна, ворующего информацию IcedID, с URL-адресами Google.

Формы «связаться с нами» на веб-сайте компании - это открытая дверь в Интернет, и преступники недавно начали использовать их для связи с работниками, которые получают запросы на контакт от общественности.

Примечательной особенностью атаки является то, что мошенники используют контактные формы для отправки сотрудникам законных URL-адресов Google, которые требуют от пользователей входа в систему с их именем пользователя и паролем Google.

Microsoft сочла угрозу достаточно серьезной, чтобы сообщить об атаках службам безопасности Google, чтобы предупредить их о том, что киберпреступники используют законные URL-адреса Google для доставки вредоносного ПО. URL-адреса Google полезны для злоумышленников, поскольку они обходят фильтры безопасности электронной почты. Похоже, что злоумышленники также обошли вызовы CAPTCHA, которые используются для проверки того, отправлено ли сообщение о контакте от человека.

«Злоумышленники злоупотребляют законной инфраструктурой, такой как контактные формы веб-сайтов, для обхода средств защиты, что делает эту угрозу очень уклончивой. Кроме того, злоумышленники используют законные URL-адреса, в данном случае URL-адреса Google, которые требуют, чтобы цели входили в систему с их учетными данными Google», - Примечания к группе аналитики угроз Защитника Microsoft 365.

Microsoft обеспокоена используемой техникой и в настоящее время обнаружила преступников, использующих URL-адреса в электронной почте для доставки вредоносного ПО IcedID. Но с таким же успехом его можно использовать для передачи других вредоносных программ.

IcedID - это банковский троян и кража информации, который может использоваться в качестве точки входа для последующих атак, например, программ- вымогателей, управляемых вручную, для особо ценных целей. Атаки программ-вымогателей, управляемые человеком, становятся все более распространенными и требуют, чтобы злоумышленник сидел за клавиатурой и организовывал атаку, в отличие от автоматизированной атаки.

«Мы уже предупредили группы безопасности в Google, чтобы они привлекли внимание к этой угрозе, поскольку она использует URL-адреса Google», - заявили в Microsoft.

«Мы наблюдали приток электронных писем с контактными формами, нацеленных на предприятия посредством злоупотребления контактными формами компаний. Это указывает на то, что злоумышленники могли использовать

инструмент, который автоматизирует этот процесс, обходя защиту CAPTCHA», - добавили в компании.

Это сложная атака, которую компании и государственные учреждения могут обнаружить, поскольку электронное письмо приходит к сотрудникам из их собственной контактной формы и систем электронного маркетинга.

«Поскольку электронные письма отправляются из собственной контактной формы получателя на его веб-сайте, шаблоны электронной почты соответствуют тому, что они ожидают от реального взаимодействия с клиентом или запроса», - отмечает Microsoft.

Злоумышленники используют формулировки, которые заставляют сотрудника отреагировать - например, ложные утверждения о том, что целевой веб-сайт использует изображения, защищенные авторским правом. В электронном письме содержится ссылка на страницу sites.google.com, где сотрудник должен просматривать изображения, предположительно нарушающие авторские права.

Если сотрудник выполняет свою работу и исследует претензию, войдя на сайт, страница sites.google.com автоматически загружает ZIP-файл с файлом JavaScript, который, в свою очередь, загружает вредоносное ПО IcedID в виде файла.DAT. Он также загружает компонент набора для тестирования на проникновение, Cobalt Strike, который позволяет злоумышленнику управлять устройством через Интернет». ***(Liam Tung. Criminals spread malware using website contact forms with Google URLs // ZDNet (https://www.zdnet.com/article/criminals-spread-malware-using-website-contact-forms-with-google-urls/). 12.04.2021).***

***

«Время, которое киберпреступники проводят внутри взломанных сетей, сокращается. Но хотя это может показаться положительным сдвигом, одна из причин, по которой хакеры проводят меньше времени внутри сетей, - это рост числа атак программ-вымогателей.

Исследователи из компании FireEye Mandiant, занимающейся кибербезопасностью, проанализировали сотни киберинцидентов и обнаружили, что глобальное среднее время ожидания - продолжительность между началом вторжения в систему безопасности и моментом его обнаружения - впервые снизилось до менее месяца и составляет 24 дня.

Согласно ежегодному отчету об угрозах M-Trends 2021, это означает, что инциденты выявляются в два раза быстрее, чем в прошлом году, когда среднее время ожидания составляло 56 дней - и намного быстрее, чем десять лет назад, когда это часто происходило. год, чтобы организации осознали, что киберпреступники проникли в сеть.

Хотя отчасти это сокращение времени ожидания происходит благодаря улучшенным возможностям обнаружения и реагирования со стороны организаций, рост числа программ- вымогателей также сыграл свою роль.

Атаки программ-вымогателей становятся все более опасной проблемой кибербезопасности, поскольку киберпреступники проникают в сети, компрометируют все, что могут, с помощью вредоносных программ для

шифрования файлов, а затем требуют выкупа - чаще всего в биткойнах - в обмен на восстановление сети.

Атаки очень прибыльны для киберпреступников, но, в отличие от большинства других форм кибер-атак, программы-вымогатели не остаются незамеченными - жертвы атак программ-вымогателей знают, что они стали жертвой, когда их сеть внезапно зашифровывается, а записка о выкупе остается нападающие.

Одним из ключевых преимуществ атак программ-вымогателей для киберпреступников является то, что они могут принести им много денег за относительно короткий промежуток времени. После того, как они скомпрометировали все необходимые активы в сети, нет смысла ждать, поэтому злоумышленники выполнят атаку программы-вымогателя как можно быстрее.

Пока атаки программ-вымогателей остаются успешными, нет оснований полагать, что киберпреступники перестанут запускать их против организаций с уязвимыми сетями.

«Расширение программ-вымогателей демонстрирует, что оно полезно для злоумышленников. Проще говоря, злоумышленники будут действовать таким образом, чтобы воздействовать на их мотивацию», - сказал ZDNet Стивен Стоун, старший директор по передовым методам работы в Mandiant.

«Все больше и больше злоумышленников используют программы-вымогатели для самых разных целей. Мы ожидаем, что это разнообразие сохранится со временем и обеспечит более сложные вторжения в 2021 году».

Программы-вымогатели - не единственная угроза, с которой сталкиваются организации: киберпреступники, например, продолжат попытки взломать сети с помощью фишинговых и вредоносных кампаний.

Хотя возможность быстро обнаруживать атаки внутри сети лучше, чем не обнаруживать их вообще, лучший способ защитить организацию от киберугроз - это обнаруживать или предотвращать их до того, как у них появится возможность взломать сеть.

Чтобы помочь в этом, отчет FireEye Mandiant рекомендует основы безопасности, включая управление уязвимостями и исправлениями, чтобы кибератаки не могли воспользоваться известными уязвимостями в сетях». ***(Danny Palmer. Cybersecurity: Victims are spotting cyberattacks much more quickly - but there's a catch // ZDNet (https://www.zdnet.com/article/cybersecurity-organisations-are-getting-quicker-at-discovering-cyber-attacks-in-their-networks-but-theres-a-catch/). 13.04.2021).***

***

«Совет, оставшийся без онлайн-сервисов на несколько недель после кибератаки, должен получить от правительства 3,68 миллиона фунтов стерлингов для покрытия расходов на восстановление своих систем.

Атака обошлась Redcar and Cleveland Council в 10 миллионов фунтов стерлингов, а оставшуюся часть счета пришлось оплатить властям.

В нем говорилось, что хакерам не выплачивали выкуп.

Критики заявили, что правительство должно покрыть большую часть затрат.

Эксперты из Национального центра кибербезопасности Великобритании (NCSC) должны были быть привлечены, чтобы помочь восстановить записи на прием, документы по планированию, рекомендации по социальному обеспечению и системы подачи жалоб муниципальных властей, которые были отключены в феврале прошлого года.

'Обманутые' по урегулированию

Совет заявил, что деньги, которые будут предоставлены правительством, помогут пополнить его резервы, которые были использованы для восстановления его онлайн-систем.

Он отказался сообщить, будут ли затронуты какие-либо услуги в результате покрытия оставшейся части счета.

Лидер Совета Мэри Лэниган, возглавляющая коалицию независимых и либерал-демократов, сказала: «Мы рады, что правительство признало уникальные обстоятельства, при которых мы запросили поддержку, и выделило грант, правильно отличив преступную атаку с использованием программ-вымогателей, от которой пострадал совет, от пакеты финансовой помощи некоторых других местных органов власти, которым было предоставлено разрешение на получение займа.

«Этим преступникам не было передано никаких денег, и мы продолжаем надеяться, что в конечном итоге они будут привлечены к ответственности».

Депутат Мидлсбро Южного и Восточного Кливленда Саймон Кларк, консерватор, охарактеризовал урегулирование как «исключительно щедрое».

Товарищ Тори Джейкоб Янг, член парламента от Redcar, сказал, что это «каким-то образом восстановит удар по финансам совета».

Однако бывший лидер совета Сью Джеффри из лейбористской партии заявила, что жителей «обманом заставили думать, что они заключили выгодную сделку», поскольку им была предоставлена лишь «небольшая часть поддержки, которую им обещали правительство и местные депутаты-консерваторы». ***(Redcar cyber-attack: Government to help cover costs // BBC (https://www.bbc.com/news/uk-england-tees-56668176). 08.04.2021).***

***

«Резкое увеличение количества атак на тему COVID, трояны PowerShell, а также компрометация SolarWinds и продолжающееся распространение вредоносного ПО Sunburst стали основными причинами значительного скачка числа наблюдаемых атак в дикой природе во второй половине 2020 года, которые, по словам McAfee, усреднены. 588 атак в минуту в его телеметрии в течение третьего и четвертого кварталов 2020 года.

В последнем отчете McAfee об угрозах говорится, что в четвертом квартале исследователи наблюдали в среднем 648 угроз в минуту в реальных условиях, что на 10 процентов больше по сравнению с третьим кварталом, что является продолжающейся тенденцией к росту с 40-процентного скачка по сравнению со вторым кварталом 2020 года.

Атаки, связанные с COVID-19, продолжали оставлять свой след в экосистеме: «Глобальная сеть McAfee, насчитывающая более миллиарда датчиков,

зафиксировала 605-процентное увеличение общего количества обнаруженных угроз, связанных с COVID-19, во втором квартале», - говорится в отчете.

«Мир - и предприятия - адаптировались к пандемическим ограничениям и устойчивым удаленным вызовам, в то время как угрозы безопасности продолжали усложняться и увеличиваться в объеме», - говорится в отчете. «Несмотря на то, что значительный процент сотрудников стал более опытным и продуктивным, работая удаленно, предприятия пережили более гибкие кампании, связанные с COVID-19, среди нового состава схем« плохих актеров». Известные кампании, такие как Sunburst и новые тактики вымогателей, не оставили SOC [центров безопасности] времени на отдых».

Угрозы PowerShell выросли на 208%

Команда исследователей безопасности также зафиксировала 208-процентный рост угроз PowerShell с 3 по 4 квартал 2020 года, в первую очередь Donoff, скрытого загрузчика троянских программ, который использует макросы в файле, чтобы проскользнуть мимо средств защиты от вирусов.

Кроме того, количество вредоносных программ, нацеленных на Office, выросло на 199 процентов, а количество наблюдаемых мобильных вредоносных программ - на 118 процентов благодаря SMS Reg и другим, пояснила команда McAfee.

Немного хороших новостей для пользователей Mac: уровни вымогателей EvilQuest вернулись на землю после колоссального 420-процентного скачка в третьем квартале 2020 года; а количество обнаруженных вредоносных программ Coin Miner упало на 35 процентов в четвертом квартале.

CryptoDefense увеличила количество программ- вымогателей на 69 процентов с третьего по четвертый квартал с помощью REvil, Thanos, Ryuk и Maze, которые, помимо других атак, атаковали бренд бытовой электроники Cannon прошлым летом.

«Если мы посмотрим, в частности, на четвертый квартал 2020 года, многие нарушения, связанные с программами-вымогателями, произошли с уязвимостями в «периферийных» устройствах, которые обеспечивали безопасность компаний», - сказал Threatpost Кристиан Бик, ведущий ученый McAfee. По словам Бика, его команда также внимательно следит за ростом «инсайдерских» угроз внутри самих компаний.

Продажи удаленного доступа к взломанным системам также растут.

«Преступники предлагают деньги за доступ к компаниям», - добавил Бик. «Я бы посоветовал компаниям поддерживать политику безопасного удаленного доступа, включая управление исправлениями, двухфакторную аутентификацию, изоляцию зон и строгие политики доступа для тех, кому нужен удаленный доступ». ***(Becky Bracken. COVID-Related Threats, PowerShell Attacks Lead Malware Surge // Threatpost (https://threatpost.com/mcafee-covid-rpowershell-malware-surge/165382/). 13.04.2021).***

***

«Умные киберпреступники охотятся за веб-серверами и браузерами больше, чем за отдельными лицами. К сожалению, эти типы атак часто

игнорируются, так как их сложнее проверить (с точки зрения проверки на проникновение).

Поскольку большая часть мира теперь работает удаленно, эта угроза усилилась. Злоумышленники используют электронную почту, мгновенные сообщения, SMS-сообщения и ссылки в социальных сетях, чтобы обманом заставить домашних работников установить вредоносное ПО, которое приводит к краже личных данных, потере собственности и, возможно, проникновению в корпоративную сеть. Фишинговые атаки могут привести пользователей на поддельные сайты или целевые страницы с тем же намерением.

С какими рисками в последнее время сталкиваются организации и что можно сделать сейчас, чтобы от них защититься?

Веб-фишинг набирает обороты

В индустрии кибербезопасности наблюдается значительный всплеск веб-фишинга, начиная с семейства киберугроз HTML / фишинга. Подобные двоюродные братья HTML - / ScrInject (атаки с использованием сценариев браузера) и / REDIR (схемы перенаправления браузера) - также способствовали увеличению попыток фишинга в 2020 году. Вредоносные программы на базе Интернета имеют тенденцию отменять или обходить большинство распространенных антивирусных (AV) программ, давая ему больше шансов на выживание и успешное заражение.

Это свидетельствует о сильном интересе киберпреступников к атакам на пользователей там, где они часто наиболее уязвимы и легковерны: просмотр веб-страниц. Сочетание удаленной работы и покупок в Интернете значительно усиливает эту угрозу. Например, в прошлом году в «черную пятницу» покупатели потратили рекордные 9 миллиардов долларов. С учетом риска COVID-19, связанного с личными покупками, Киберпонедельник 2020 года, как сообщается, стал крупнейшим днем онлайн-продаж за всю историю. Веб-вредоносные программы могут скрывать и / или обходить традиционные антивирусные продукты, повышая вероятность успешного заражения.

Браузеры: ключевой вектор распространения вредоносного ПО

Браузеры непросто защитить, а веб-приложения сложно контролировать. Это некоторые из причин, по которым браузер стал ключевым вектором распространения вредоносных программ за последний год, и эта тенденция, вероятно, сохранится и в следующем году. Это соответствует зарегистрированному падению корпоративного веб-трафика, который обычно проверялся и очищался, и росту домашнего веб-трафика из-за перехода к удаленной работе.

Этот сдвиг подтверждает мысль о том, что киберпреступники намеренно изменили свои методики атак, чтобы нацелить трафик, который сейчас наводняет менее защищенные сети. Тенденции вредоносного ПО отражают намерения и возможности злоумышленников. Подобно обнаружению системы предотвращения вторжений (IPS), вредоносное ПО, обнаруженное датчиками безопасности, не всегда указывает на подтвержденное заражение, а скорее указывает на использование и / или распространение вредоносного кода. Обнаружения могут происходить на уровне сети, приложения и хоста на многих различных устройствах.

Какие действия в области кибербезопасности мне следует предпринять сейчас?

При разработке стратегии кибербезопасности организациям необходимо учитывать три момента:

Кибергигиена является ключевым моментом: организации должны предоставлять удаленным сотрудникам знания и обучение, необходимые для защиты своих личных сетей и подключенной бизнес-сети. Это включает в себя обучение, а также руководство по обновлению программного обеспечения.

Организации не могут полагаться на личную безопасность сотрудников: они также должны предоставлять дополнительные ресурсы, такие как решения для обнаружения и реагирования конечных точек (EDR), которые могут обнаруживать и блокировать сложные угрозы. Организациям необходима расширенная защита от угроз в режиме реального времени для конечных точек как до, так и после заражения.

Эффективная кибербезопасность требует постоянной бдительности и способности адаптироваться к изменяющимся стратегиям угроз: хотя безопасность всегда должна была быть главным приоритетом, возможно, сейчас самое время подумать об инвестировании в более широкие, более продвинутые, адаптируемые и интегрированные решения, особенно когда киберпреступники изменяют свои методы атак. использовать личные устройства в качестве трамплина для корпоративных сетей. Имея это в виду, укрепление удаленных систем и сетей должно занимать первое место в списке дел по обеспечению безопасности.

Пребывание в хорошем состоянии

Ландшафт угроз постоянно меняется, требуя от специалистов по безопасности быть в курсе новых типов и векторов угроз. Опытные защитники должны отметить, что браузер был основным вектором распространения вредоносных программ в 2020 году - и, вероятно, снова будет в этом году - и действовать соответствующим образом, чтобы обеспечить единообразный контроль для удаленных систем. Независимо от состояния окружающего мира, лучший способ защиты от постоянно развивающейся вредоносной активности - это комплексный и комплексный подход к кибербезопасности.

Важнейшие компоненты этого подхода включают постоянный доступ к актуальной информации об угрозах и обучение кибербезопасности для всех сотрудников, особенно тех, кто работает удаленно. Также важно использовать обновленную технологию безопасности, такую как EDR, которая обнаруживает и блокирует сложные угрозы в режиме реального времени. Весь интеллект в мире не принесет никакой пользы организации, если ее инструменты безопасности не смогут использовать ее для обнаружения и смягчения атак. Убедитесь, что все эти тактики являются частью вашей комплексной стратегии безопасности». ***(Aamir Lakhani. How To Defend the Extended Network Against Web Risks // Threatpost (https://threatpost.com/how-to-defend-the-extended-network-against-web-risks/165236/). 05.04.2021).***

***

«Академический исследователь проанализировал более 100 случаев, связанных с Законом о неправомерном использовании компьютеров, чтобы нарисовать картину преступников с компьютерами, которые не только преследовали британские действия в сфере цифровых технологий в 21 веке, но и были пойманы на этой уловке.

Как выяснил Джеймс Кроуфорд из Royal Holloway, Лондонский университет, средний осужденный по Закону о неправомерном использовании компьютеров, скорее всего, будет человеком со средней или низкой квалификацией, в основном работающим в одиночку и, скорее всего, не знающим о своей жертве.

В «техническом отчете», посвященном анализу публично зарегистрированных случаев за десять лет, Кроуфорд рассмотрел очевидные навыки мошенников, попавших в ловушку властей в соответствии с Законом о неправомерном использовании компьютеров (CMA), прежде чем исследовать их мотивацию и демографические данные.

«Категория с низким уровнем квалификации в основном состоит из бывших ИТ-сотрудников, которые использовали свои знания систем, которые они использовали, чтобы нанести ущерб своим предыдущим работодателям», - отметил Кроуфорд, который привел в пример негодяя из Jet2 Скотта Бернса.

Действительно, большое количество цитат из его статьи связано с отчетами The Register о случаях CMA за эти годы.

По данным, проанализированным Кроуфорд, на мужчин приходилось 97 процентов преступников, причем только три преступника из 100 были женщинами. «Средний возраст тех, кто считается хакерами в этом проекте, составляет чуть более 29 лет на момент вынесения приговора. Самому молодому хакеру, участвовавшему в опросе, было 16 обвинительных приговоров (14 на момент совершения преступлений). Самому старшему было 69».

Тем не менее, средний преступник, злоупотребляющий компьютерами, - это «молодой мужчина с преобладанием психических расстройств и нарушений развития», - заключил исследователь.

Закон используется не так часто

Кроуфорд также был менее чем позитивен в отношении использования CMA в качестве инструмента правоохранительных органов, заявив: «… можно с уверенностью сделать вывод, что CMA зафиксировало в общей сложности восемь обвинительных приговоров для хакеров, продемонстрировавших высокий уровень навыков (или по крайней мере, не более восьми).

«Это не особенно впечатляющая отдача от CMA за 12 лет, особенно с учетом того внимания, которое уделялось киберпреступности за этот период (с учетом того факта, что высококвалифицированные хакеры могли быть осуждены в соответствии с отдельным законодательством)».

С другой стороны, британские полицейские силы были довольно хорошо отвлечения молодых компьютерных позволили преступникам в мероприятиях, позволяющих объединить свои таланты позитивные вещи, такие как работа в ИТ - индустрии.

Относительно низкая частота судебных преследований CMA соответствует тому, что ваш корреспондент видел в судах. Часто преступления, совершенные с

помощью компьютеров, могут преследоваться по закону о мошенничестве, и прокуроры находятся под постоянным (и правильным) давлением, чтобы они выдвинули обвинения с наибольшей вероятностью обвинительного приговора. CMA, в котором нет конкретных руководящих принципов вынесения приговоров, может быть менее привлекательным вариантом, когда судье или присяжным можно рассказать прямую историю об обмане вместо того, чтобы потенциально выслушать массу технического жаргона.

Кроуфорд также отметил, что в период с 2008 по 2020 год было возбуждено 172 дела CMA без какой-либо PR-активности со стороны СМИ или полиции. Не имея легкодоступных доказательств в открытом доступе, он не смог проанализировать эти случаи. Его отчет можно прочитать здесь [PDF].

Статистика скомпилированная по The Register лета 2019 года показала, что в период с 2008 по 2018 год в общей сложности 422 людей были обвинены в совершении преступлений, CMA, из которых 343 были признаны виновными. Из числа виновных 135 были оштрафованы или приговорены к судебному приказу, а 157 - к тюремному заключению с отсрочкой исполнения или немедленным лишением свободы.

За тот же 10-летний период было вынесено 644 предупреждения за нарушение CMA, что говорит о том, что полиция была готова нанести киберпреступникам заслуженную пощечину». ***(Gareth Corfield. Average convicted British computer criminal is young, male, not highly skilled, researcher finds // The Register (https://www.theregister.com/2021/04/13/uk_computer_misuse_act_conviction_analysis/). 13.04.2021).***

***

«Исследователи безопасности отмечают рост числа альтернативных методов кражи данных от фишинговых атак, поскольку мошенники получают украденную информацию через Google Forms или частных ботов Telegram.

Электронная почта остается предпочтительным методом кражи украденной информации, но эти каналы предвещают новую тенденцию в развитии фишинговых комплектов.

Тенденции к удаленной кражи данных

Анализируя фишинговые наборы за последний год, исследователи из компании по кибербезопасности Group-IB заметили, что большее количество этих инструментов позволяет собирать украденные данные пользователей с помощью Google Forms и Telegram.

Они считаются альтернативными методами получения скомпрометированных данных и составляют около 6% от того, что обнаружили аналитики Group-IB, и эта доля, вероятно, увеличится в краткосрочной перспективе.

Хранение информации в локальном файле на фишинговом ресурсе также является частью альтернативных методов эксфильтрации и составляет самый высокий процент из всех.

Использование Telegram не новость, поскольку операторы обратились к этой услуге, поскольку она анонимна и проста в использовании. Пресловутый фишинговый комплект 16Shop имел такую возможность еще в 2019 году.

Операция жульничества, как услуга используется, по меньшей мере, 40 киберпреступными бандами олицетворять популярные объявления, а также полагались на Телеграмма ботов предоставить мошеннические веб - страниц.

Отправка украденных данных, собранных с фишингового сайта, в Google Form осуществляется с помощью POST-запроса в онлайн-форму, ссылка на которую встроена в набор для фишинга.

По сравнению с электронной почтой, которая может быть заблокирована или украдена, а журналы потеряны, это более безопасный метод эксфильтрации информации, сообщил Group – IB BleepingComputer.

Разработчики обманывают покупателей

Еще одна тенденция, которую наблюдали исследователи, заключалась в том, что авторы фишинговых комплектов дважды пытались увеличить свою прибыль, добавляя код, копирующий поток украденных данных на их сетевой хост.

Group-IB объяснила, что одним из способов является настройка функции «отправки» для доставки информации на адрес электронной почты, предоставленного покупателем комплекта для фишинга, а также переменной «токена», связанной со скрытым адресом электронной почты.

Запрос POST из сценариев, ответственных за отправку данных, также инициализирует переменную «токен». Расшифровка данных из «токена» показывает, что разработчик связал два адреса электронной почты для его значения.

Исследователи Group-IB также заметили, что разработчики фишинговых комплектов скрывают в коде веб-оболочки, предоставляя им удаленный доступ к ресурсу.

Что касается приманок, компания выявила более 260 уникальных брендов, большинство из которых предназначены для онлайн-сервисов (30,7% - онлайн-инструменты для просмотра документов, онлайн-покупок, потоковых сервисов и т. Д.), Почтовых клиентов (22,8%), и финансовые организации (20%), которые являются типичными целями.

Исследователи говорят, что основными целями были пользователи продуктов Microsoft, PayPal, Google и Yahoo.

Ярослав Каргалев, заместитель директора группы реагирования на инциденты Group-IB (CERT-GIB), говорит, что сегодня мошенники используют автоматизацию для более быстрой замены заблокированных фишинговых страниц.

Прямым следствием этого является распространение «более сложной социальной инженерии, используемой в крупномасштабных атаках», говорит Каргалев, что требует блокирования всей инфраструктуры злоумышленника, а не только фишинговых веб-сайтов». ***(Ionut Ilascu. Google Forms and Telegram abused to collect phished credentials // Bleeping Computer (https://www.bleepingcomputer.com/news/security/google-forms-and-telegram-abused-to-collect-phished-credentials/). 07.04.2021).***

***

«Недавняя фишинговая кампания использовала хитрый прием для доставки мошеннической веб-страницы, которая собирает учетные данные Microsoft Office 365, создавая ее из фрагментов HTML-кода, хранящихся локально и удаленно.

Метод состоит из объединения нескольких фрагментов HTML, скрытых в файлах JavaScript, для получения поддельного интерфейса входа в систему и предложения потенциальной жертве ввести конфиденциальную информацию.

Скрытые строительные блоки

Жертвы получили электронное письмо с вложением, в котором утверждалось, что это файл Excel (.XLSX) об инвестициях. На самом деле файл представляет собой HTML-документ с фрагментом текста в кодировке URL.

Исследователи из Trustwave расшифровали текст и обнаружили, что впереди еще больше расшифровок, поскольку он был затем запутан с помощью кодов сущностей. Используя CyberChef GCHQ, они обнаружили ссылки на два файла JavaScript, размещенных на yourjavascript.com, домене, используемом для других фишинговых кампаний.

В каждом из двух файлов JavaScript было два блока закодированного текста, скрывающего код HTML, URL и кодировку Base64.

В одном из них исследователи обнаружили начало фишинг-страницы и код, который проверяет адрес электронной почты и пароль жертвы.

Второй JavaScript содержал функцию «submit», расположенную с помощью тегов «form» и кода, который запускал всплывающее сообщение, информирующее жертв о том, что они вышли из системы и им необходимо пройти аутентификацию снова.

В целом исследователи расшифровали более 367 строк HTML-кода, разделенных на пять частей среди двух файлов JavaScript и одного вложения электронной почты, которые, собранные вместе, создали фишинговую страницу Microsoft Office 365.

Trustwave сказал, что необычность этой кампании заключается в том, что JavaScript загружается в виде запутанных фрагментов из удаленного места, а затем собирается вместе локально.

«Это помогает злоумышленникам обойти средства защиты, такие как Secure Email Gateways, которые могут идентифицировать вредоносный JavaScript из исходного вложения и блокировать его», - добавили исследователи.

Адрес электронной почты жертвы заполняется автоматически, чтобы обеспечить легитимность. Фишинговые мошенники также проверяют, не является ли пароль пустым, и используют регулярные выражения для подтверждения действительного адреса электронной почты.

В сегодняшнем сообщении в блоге Trustwave отмечает, что URL-адрес, получающий украденные учетные данные для этой кампании, все еще активен.

Исследователи говорят, что уловки в этой кампании необычны. Используя вложение HTML, указывающее на удаленный код JavaScript и уникальную кодировку, киберпреступники стараются избежать обнаружения». ***(Ionut Ilascu. Microsoft Office 365 phishing evades detection with HTML Lego pieces // Bleeping***

Computer (https://www.bleepingcomputer.com/news/security/microsoft-office-365-phishing-evades-detection-with-html-lego-pieces/). 08.04.2021).

***

«По словам представителя Европейской комиссии, в марте Европейская комиссия и несколько других организаций Европейского союза пострадали от кибератаки.

Как сообщил пресс-секретарь, «инцидент с ИТ-безопасностью» затронул ИТ-инфраструктуру нескольких институтов, органов или агентств ЕС.

«Мы тесно сотрудничаем с CERT-EU, группой реагирования на компьютерные чрезвычайные ситуации для всех институтов, органов и агентств ЕС, а также с поставщиком затронутого ИТ-решения», - сказал представитель BleepingComputer.

«Комиссия создала круглосуточную службу мониторинга и активно принимает меры по смягчению последствий».

«Серьезных утечек информации» пока не обнаружено, хотя судебно-медицинский анализ попыток вторжения все еще находится на начальной стадии, и окончательной информации нет.

«Позвольте мне воспользоваться случаем, чтобы напомнить, что мы очень серьезно относимся к кибербезопасности и применяем строгие политики для защиты нашей инфраструктуры и устройств, - добавил представитель. - Мы расследуем каждый инцидент».

На данный момент нет информации о характере инцидента или личности злоумышленников, стоящих за атакой.

Хотя это и не подтверждено представителем Европейской комиссии, агентство Bloomberg ранее сообщало, что на прошлой неделе атака нанесла ущерб организациям ЕС.

Другие организации ЕС, подвергшиеся атакам в последние месяцы

В прошлом месяце Европейскому банковскому управлению (EBA) пришлось отключить все почтовые системы после взлома их серверов Microsoft Exchange в рамках продолжающихся атак, направленных на коммерческие и правительственные организации по всему миру.

В январе Европейское агентство по лекарственным средствам (EMA) заявило, что данные о вакцине Pfizer / BioNTech COVID-19, украденные с его серверов в декабре, просочились в сеть.

В последующем обновлении EMA показало, что некоторые данные о вакцинах-кандидатах были подделаны злоумышленниками, прежде чем просочиться в сеть, чтобы подорвать доверие общественности к вакцинам COVID-19.

Исследователи IBM X-Force также предупредили в декабре об угрозах, нацеленных на организации, связанные с холодовой цепью вакцины COVID-19, включая Генеральный директорат Европейской комиссии по налогообложению и таможне Unio». ***(Sergiu Gatlan. European Commission, other EU orgs recently hit by cyber-attack // Bleeping Computer***

(https://www.bleepingcomputer.com/news/security/european-commission-other-eu-orgs-recently-hit-by-cyber-attack/). 06.04.2021).

***

«Компания Qualys, занимающаяся кибербезопасностью, заявила сегодня, что злоумышленники, взломавшие ее сервер Accellion FTA, не проникли в производственную и корпоративную среду компании.

Сторонняя судебно-медицинская фирма, нанятая для расследования того, вторглись ли хакеры в сеть Qualys сбоку, не нашла доказательств бокового движения от взломанного устройства для обмена файлами.

Qualys также отметила, что расследование показало, что «существующие правила безопасности компании не допускали такого доступа между сервером Accellion FTA и корпоративной и производственной средой Qualys.

«Как отмечалось ранее, влияние на Qualys и наших клиентов ограничивается сервером Accellion FTA», - сказал Бен Карр, директор по информационной безопасности Qualys.

«Мы по-прежнему уверены, что этот инцидент не повлияет на производственную среду Qualys (общие платформы и частные платформы), кодовую базу, данные клиентов, размещенные на облачной платформе Qualys, агенты Qualys или сканеры».

Согласно Qualys, его платформы полностью функциональны, поскольку атака не привела к простоям или операционным последствиям...

Банда вымогателей Clop опубликовала скриншоты файлов, предположительно украденных с сервера Qualys Accellion FTA после взлома сервера в декабре 2020 года. Утечка данных включала счета-фактуры, заказы на покупку, налоговые документы и отчеты о сканировании.

Qualys заявила, что затронутые серверы Accellion FTA были отключены, и компания переключилась на альтернативные решения для передачи файлов, связанных с поддержкой.

Хотя Qualys не упомянула записку о выкупе, полученную от Клопа, согласно отчету FireEye Mandiant, другие жертвы банды вымогателей получали их и раньше.

До сих пор неясно, стоит ли банда вымогателей Clop за атаками Accellion, которые она опубликовала на своем сайте утечки данных, или в партнерстве с другой группой для обмена файлами и вымогательства у жертв.

Совместное заявление, опубликованные Mandiant и Accellion пролить больше света на эти нападения, связывая их с киберпреступностью группы FIN11…». ***(Sergiu Gatlan. Qualys says Accellion hackers did not breach production systems // Bleeping Computer (https://www.bleepingcomputer.com/news/security/qualys-says-accellion-hackers-did-not-breach-production-systems/). 02.04.2021).***

***

«97% организаций в мире подвергались атакам на мобильные устройства в 2020 году, заявила компания Check Point Software Technologies Ltd, специализирующаяся на кибербезопасности.

В Mobile Security Report 2021 специалисты Check Point исследовали последние угрозы, нацеленные на корпоративные мобильные устройства, и представили обзор основных тенденций в области мобильных вредоносных программ, уязвимостей и кибератак государственного уровня…

Переход к массовой удаленной работе во время пандемии COVID-19 привел к резкому росту количества мобильных атак, в результате чего 97% организаций столкнулись с угрозами сразу с нескольких направлений, заявляет компания. Специалисты Check Point прогнозируют, что к 2024 году 60% всех офисных сотрудников станут мобильными, поэтому защита мобильных устройств должна быть приоритетом для организаций.

«Прошедший год показал, что ландшафт мобильных угроз продолжает расширяться, и сегодня практически каждая организация сталкивается с атаками», — прокомментировал Василий Дягилев, глава представительства Check Point Software Technologies в России и СНГ.

«Киберпреступники начинают активно использовать новый тренд и адаптируют под него свои методы атак, чтобы через конечные и зачастую личные мобильные устройства пользователей получать доступ к корпоративным данным. Организациям стоит серьезно задуматься и об их защите», — добавил Дягилев.

По данным Check Point, почти половина организаций в мире пострадала от вредоносных мобильных приложений: в 46% компаний по крайней мере один сотрудник загрузил вредоносное приложение в 2020 году, тем самым поставив под угрозу корпоративные данные и сеть организации в целом.

Также компания зафискировала рост числа мобильных вредоносных программ: в 2020 году активность банковских троянов, которые способны похищать учётные данные пользователей мобильного банкинга, выросла на 15%. Часто злоумышленники распространяют мобильное вредоносное ПО, в том числе трояны для удалённого доступа к мобильным устройствам (MRAT), банковские трояны и программы дозвона премиум-класса через приложения, якобы связанные с COVID-19». ***(Андрей Шляховский. 97% компаний пострадали от действий хакеров: Check Point поделилась данными о кибератаках // ООО "РБ.РУ" (https://rb.ru/news/97-check-point/). 13.04.2021).***

***

«Специалисты техногиганта Facebook обезвредили расположенную в Албании ферму троллей. Операторы фермы с помощью искусственного интеллекта создавали дипфейк-изображения и распространяли дезинформацию среди иранских пользователей. Как сообщается в отчете Coordinated Inauthentic Behavior, злоумышленники также были связаны с группой боевиков «Моджахедин-э Халк», насчитывающей несколько тысяч участников.

Группировка создавала фальшивые учетные записи для осуществления пропаганды против правительства Ирана и выдавала себя за журналистов и новостные агентства.

Национальный совет сопротивления Ирана и «Моджахедин-э Халк» организаций опровергли утверждения Facebook о существовании фермы троллей и сообщили, что никогда не создавали фейковые аккаунты на платформе.

В своем отчете Facebook также упомянула об усилиях по снижению количества злонамеренных действий в своей соцсети. По данным компании, в марте было заблокировано 1167 учетных записей в Facebook, 290 учетных записей в Instagram, 255 страниц и 34 группы из-за их связи с «кампаниями скоординированного неправомерного поведения», нацеленными на Израиль, Мексику, Грузию и пр». ***(Facebook обезвредила ферму троллей в Албании // SecurityLab.ru (https://www.securitylab.ru/news/518946.php). 15.04.2021).***

***

«Когда американским компаниям становится известно о том, что их атаковали киберпреступники или финансируемые правительствами хакеры, они должны сообщать об этом властям и предоставлять им всю необходимую информацию, которая может помочь правительству лучше сдерживать атаки так называемых «государственных» хакеров. Об этом сообщил директор ФБР Кристофер Рэй (Christopher Wray), выступая перед Конгрессом США.

По словам Рэя, правильное поведение компаний, ставших жертвами кибератак, поможет правительству разработать своего рода систему раннего предупреждения об атаках иностранных хакеров, проводящих широкомасштабные кибероперации против множества американских компаний и государственных структур. Как пояснил глава ФБР, очень важно выявить организацию, ставшей первой жертвой в череде кибератак иностранных хакеров, чтобы можно было предотвратить дальнейшее распространение угрозы.

Подобные предупреждения со стороны частного сектора уже помогали правительству США узнавать о вредоносных операциях, финансированных иностранными государствами. К примеру, ИБ-компания FireEye, ставшая одной из жертв взлома SolarWinds в декабре 2020 года, является первой организацией, сообщившей об этом. Именно отчет FireEye положил начало процессу, который помог правительству и другим компаниям выявить взломы своих систем.

Многие лидеры разведывательного сообщества США, выступавшие перед Конгрессом наряду с Рэем, в том числе директор Национальной разведки Аврил Хэйнс (Avril Haines) и директор Агентства национальной безопасности Пол Накасоне (Paul Nakasone), поддержали настойчивые требования директора ФБР по укреплению партнерства между государственным и частным сектором в вопросе выявления таких взломов.

Накасоне отметил, что в случаях, когда для проведения своих операций иностранные национальные государства или киберпреступники используют инфраструктуру США, американская разведка может отставать от того, что может увидеть частный сектор, поскольку она зачастую не имеет права осуществлять мониторинг таких атак быстро». ***(Глава ФБР попросил частные компании сообщать о хакерски х атаках // SecurityLab.ru (https://www.securitylab.ru/news/518963.php). 15.04.2021).***

***

«Как сообщает компания Beaming, в первые три месяца 2021 года британские компании стали жертвами кибератак, число которых увеличилось на 11% по сравнению с предыдущим годом.

В течение первого квартала британские компании потерпели более 172.000 атак, что составляет примерно 1912 атак каждый день. А попытки атаки совершались каждые 45 секунд. Для сравнения в 2020 году в первом квартале на день приходилось примерно 1725 атак.

Вполне вероятно, что большинство этих атак были автоматизированными и организации с надежной кибербезопасностью могли их легко отразить.

Злоумышленники чаще всего атаковали устройства интернета вещей и сервисы для совместного использования файлов. На них пришлось 175 и 100 атак в день соответственно.

IP-адреса чаще всего были из Китая (14%), США (11%) и Индии (6%)». ***(Компании Великобритании стали жертвами рекордного количества кибератак в первые три месяца 2021 года // SecureNews (https://securenews.ru/uk-companies-have-been-the-victims-of-a-record-number-of-cyber-attacks-in-the-first-three-months-of-2021/). 09.04.2021).***

***

«Пользователей LinkedIn атаковали фишинговыми сообщениями в попытке «угнать» их аккаунты или продвинуть фейковые электронных адреса.

Согласно Bitdefender Antispam Lab, новые кампании по рассылке спама являются последствием утечки данных пользователей LinkedIn. Хотя рассылка спама не может быть связана напрямую с утечкой данных 500 млн пользователей платформы, огромное количество мошеннических электронных писем говорит об обратном.

Bitdefender Antispam Lab обнаружила более 500 млн вредоносных сообщений, которые рассылались premium-пользователям из США, ОАЭ, стран ближнего Востока и Канады.

Скамеры не запрашивали личную информацию и не прикрепляли вредоносные вложения. Вместо этого, в конце каждого сообщения была кнопка «Отписаться», которая вела на подозрительные домены». ***(Утечка данных в LinkedIn: сотни тысяч сообщений со спамом заполнили почты пользователей // SecureNews (https://securenews.ru/linkedin-data-leak-hundreds-of-thousands-of-spam-messages-filled-users-emails/). 15.04.2021).***

***

«Исследователи Check Point Research представили отчет за первый квартал о брендах, которые чаще всего использовались в фишинговых атаках. В таких атаках злоумышленники, пытаясь втереться в доверие к пользователям, имитируют официальный сайт известной компании, используя доменное имя, URL-адрес и дизайн, аналогичные оригинальным.

Жертвы могут получить ссылку на поддельную страницу по электронной почте или SMS. Также они могут быть перенаправлены на фишинговый сайт во

время просмотра страниц в сети или из вредоносного мобильного приложения. Фейковые сайты часто содержат форму, предназначенную для кражи учетных или платежных данных, а также другой личной информации.

Как и ранее, чаще всего мошенники использовали бренд Microsoft – 39% всех попыток фишинга с упоминанием известных компаний были связаны с этим технологическим гигантом (немного меньше, чем в четвертом квартале – тогда этот показатель составил 43%). Таким образом, киберпреступники все еще нацелены на работающих удаленно. В целом представители отрасли высоких технологий преобладают в рейтинге.

Второе место сохраняет компания DHL (18% всех попыток) – хакеры продолжают эксплуатировать растущий спрос на покупки в Сети.

На третьей позиции банковская сфера в лице Wells Fargo и Chase потеснила розничную торговлю. То есть мошенники используют рост цифровых платежей, зависимость от онлайн-банкинга, покупок в сети и доставки на дом.

В связи с этим специалисты неустанно призывают пользователей быть предельно аккуратными и внимательными при передаче личных и учетных данных и дважды думать, прежде чем открывать вложения электронной почты или ссылки.

Топ брендов, которые чаще всего использовали злоумышленники: Microsoft (39% всех попыток фишинговых атак с использованием названий брендов в мире), DHL (18%), Google (9%), Roblox (6%), Amazon (5%), Wells Fargo (4%), Chase (2%), LinkedIn (2%), Apple (2%), Dropbox (2%)». ***(Microsoft остается излюбленным брендом организаторов фишинговых атак // Компьютерное Обозрение (https://ko.com.ua/microsoft_ostaetsya_izlyublennym_brendom_organizatorov_fishingovyh_atak_137070). 16.04.2021).***

***

«Фахівці міжнародного розробника антивірусного програмного забезпечення, експерта у сфері кіберзахисту-компанії ESET попередили про зростання кількості кібератак на державні установи на тлі пандемії, розповіли про види подібних атак і дали поради, як захиститися від зловмисників.

"Більш поширеними стають кібератаки, метою яких є перешкода наданню послуг, викрадення даних або компрометація стратегічної національної інфраструктури. Серед найбільш відомих інцидентів за останній час - злом SolarWinds Orion, несанкціоноване використання Microsoft Exchange, атаки на інструмент моніторингу IT –інфраструктури Centreon і на системи охорони здоров'я у Франції та Німеччині, а також збільшення кількості атак на школи, університети та освітні IT - платформи», - повідомляють в компанії ESET.

Фахівці з кібербезпеки очікують, що кіберзлочинці продовжать вдосконалювати свої тактики, використовуючи тему COVID-19 і націлюючись на поширені програми.

Інструменти кібершпіонажу

Як зазначають в ESET, сновними цілями шпигунських операцій є великі організації та державні установи, такі як міністерства закордонних справ, посольства та інші дипломатичні представництва. Для викрадення конфіденційної інформації зловмисники використовують різні способи атак, спільною особливістю

яких є прихована активність, що дозволяє їм залишатися непоміченими в мережі жертв якомога довше.

"Прикладом такої шкідливої програми є новий бекдор Crutch для крадіжки документів, який належить відомій групі кіберзлочинців Turla. Дослідники ESET виявили Crutch в мережі Міністерства закордонних справ однієї з країн Європейського Союзу. Крім цього, APT-група Turla використовує і інші витончені інструменти. Серед них - безфайлові загрози, наприклад, завантажувач PowerShell з відкритим вихідним кодом для запобігання виявлення, а також шкідлива програма LightNeuron, націлена на сервери Microsoft Exchange», - повідомляють фахівці.

Згідно з повідомленням, ще однією небезпечною групою кіберзлочинців є Gamaredon, яка відома своїми атаками на державні установи в Україні. Ця група додає шкідливі макроси в документи Microsoft Word і Excel, таким чином поширюючи загрози. Використовуючи легітимні інструменти, які застосовуються в державних і бізнес-структурах, Gamaredon швидко знаходить доступні конфіденційні дані і далі поширюється в мережі.

Програми-вимагачі

За даними ESET, однією з найнебезпечніших загроз для державних установ є потрапляння в їхню мережу програм-вимагачів, які шифрують важливі дані і вимагають великі суми за їх розблокування.

Зокрема, в жовтні 2020 року фахівці ESET у співпраці з Microsoft і декількома правоохоронними установами, викрили ботнет Trickbot, за допомогою якого зловмисники не тільки викрадали гроші з банківських рахунків, але і заражали організації, розгортаючи програму-вимагач Ryuk і вимагаючи викуп.

Згідно телеметрії ESET, зі зниженням активності Trickbot кількість виявлених зразків ботнету Emotet збільшувалася. Зв'язок між цими двома загрозами дозволив знешкодити в січні 2021 року і Emotet в ході масштабної операції Європолу і ряду правоохоронних органів в Європі і Північній Америці.

У компанії ESET зазначають, що такі групи кіберзлочинців можуть тижнями або місяцями збирати інформацію в заражених системах і тільки після цього розгортати програми-вимагачі. Деякі кіберзлочинці таким чином намагаються отримати прибуток, інші ставлять собі за мету підірвати довіру до державних установ у певній країні.

Атака на розробників програм

Як попереджають експерти у сфері кіберзахисту, цифровізація і вигоди від співпраці з сторонніми постачальниками збільшили ризик атак на розробників програмного забезпечення, мета яких полягає в додаванні шкідливого коду в безпечну програму і поширенні його серед усіх користувачів (атаки ланцюг поставок). Зокрема, нещодавно в центрі уваги опинилася компрометація програмного забезпечення SolarWinds Orion. Під загрозою опинилися тисячі користувачів цієї платформи, а зловмисники і APT-групи отримали можливості для широкомасштабної активності.

Крім цього, дослідники ESET за останні кілька місяців виявили кілька інших атак на ланцюг поставок - від використання зламаних додаткових інструментів безпеки для поширення шкідливого коду до атак на корпоративне програмне

забезпечення для чатів, а також від компрометації центру сертифікації до зараження емулятора Android.

У компанії прогнозують, що, враховуючи складність виявлення таких атак і їх прибутковість для кіберзлочинців, їх кількість продовжить збільшуватися найближчим часом у всьому світі.

Робота з дому

За даними ESET, перехід на віддалений режим роботи призвів до зростання ризиків для всіх роботодавців, а, отже, і державних установ.

Як повідомляють фахівці, 23% інцидентів кібербезпеки сталися через помилки персоналу. Зловмисники часто користуються інтуїтивним бажанням користувачів швидко перейти за посиланням, яке виглядає як безпечне. Однак, деякі з найбільших порушень були викликані діями досвідчених IT-фахівців, зокрема, через підключення персональних пристроїв співробітників до корпоративних систем, неправильного налаштування хмарних систем та інших помилок.

Захист від новітніх векторів атак: з чого почати

Як повідомляють в ESET, установи вже зараз можуть підготуватися до сучасних векторів атак за допомогою багаторівневої системи безпеки.

Згідно з повідомленням, захистити від "0-денних" загроз допоможе хмарна пісочниця, а повний огляд активності робочих станцій і своєчасне реагування на інциденти забезпечить EDR-рішення. Від витоків даних захистить рішення для запобігання втрати даних, яке допоможе виявляти підозрілі дії з конфіденційною інформацією. Крім цього, важливо також забезпечити регулярне оновлення програмного забезпечення, резервне копіювання і захист робочих станцій.

"За підсумками минулого року однією з позитивних тенденцій в кібербезпеці, як і в боротьбі з коронавірусом, є поява міцного партнерства між державними органами і приватним сектором для вирішення актуальних проблем. Компанія ESET розуміє важливість такої взаємодії і готова співпрацювати з державними органами для поліпшення безпеки цифрового світу», - підсумували в компанії…» ***(Ірина Погоріла. Фахівці попереджають про зростання кількості кібератак на держустанови // УНІАН (https://www.unian.ua/politics/fahivci-poperedzhayut-pro-zrostannya-kilkosti-kiberatak-na-derzhustanovi-novini-ukrajina-11406361.html?_gl=1*1jtdoe3*_ga*NDY3NTk3NDU0LjE2MTg4Mzg2NjU.*_ga_JLSK4Y8K67*MTYxOTc4NDYxMi4yLjEuMTYxOTc4NDg3MC42MA..*_ga_DENC12J6P3*MTYxOTc4NDYxMi4yLjEuMTYxOTc4NDg3MC42MA..). 30.04.2021).***

***

«Внедрение Интернета и его быстрый рост в 1990-х и 2000-х годах не только изменили наше общество, но и коренным образом изменили то, как работают как малые, так и крупные предприятия. Технологии расширились и приблизили нас к более крупным рынкам. Преступники тоже нашли свое место в этой экосистеме. Система уголовного правосудия и правоохранительные органы не были предназначены для борьбы с этим видом преступлений. Лишь три десятилетия спустя были созданы основы и ресурсы для эффективного

противодействия киберпреступникам. Компании начинают рассматривать киберпреступность как серьезную угрозу.

Теперь мы хорошо осознаем его разрушительный потенциал и начинаем признавать постоянный характер киберпреступности. Исторически жертвами стали банки, национальные парламенты и крупные производственные конгломераты. У киберпреступников есть разные мотивы для растущего числа атак: финансовая выгода, политические манипуляции и финансирование преступной деятельности. Правительство Люксембурга подготовило последнюю версию Национальной стратегии кибербезопасности в 2018 году. Угроза не является теоретической. В конце 2020 года крупный люксембургский PSF (профессиональный финансовый сектор) был атакован хакерами, что привело к серьезным сбоям в работе. Это не был единичный инцидент.

Для финансового сектора Люксембурга киберугроза присутствует постоянно.

С точки зрения регуляторов недостатка в рекомендациях по определению киберпреступности как риска нет. Европейское банковское управление и Европейский центральный банк определили ИТ и кибер-риски как серьезные угрозы, особенно с учетом того, что большинство этих функций в индустрии финансовых услуг передаются на аутсорсинг. Люксембургский CSSF недавно обновил свое руководство, среди прочего, по управлению рисками в своем Циркуляре 12/552, который устанавливает минимальные требования к надзору для большей части отрасли. Особое внимание уделяется управлению рисками в рамках регулируемых организаций, надлежащей идентификации и управлению ИТ-рисками, а также надлежащему надзору и обучению членов совета директоров.

Сдерживайте киберпреступников - используйте проактивную стратегию

В конечном итоге именно отдельные члены совета директоров несут ответственность за управление ИТ-рисками и предотвращение кибератак. Вероятно, благодаря опыту и знаниям этих высших руководителей большинство люксембургских организаций смогли эффективно отреагировать на пандемию, с относительной легкостью переключившись на удаленные процессы и операции. Для многих это означало обновление застойного присутствия в сети у клиентов или выделение последнего раунда финансирования долгожданного обновления ИТ. Тем, кто осознал эту необходимость на раннем этапе кризиса, удалось сохранить операционную устойчивость и непрерывность бизнеса. Многие другие обнаружат, в какой степени они передали ИТ на аутсорсинг или полагались на критически важные функции в своей группе.

Эти навыки не следует путать с опытом и подготовкой, необходимыми для оценки киберрисков и защиты от них.

Финансовым учреждениям необходимо срочно пересмотреть набор навыков членов совета директоров. Недостаточно полагаться на одного члена совета директоров с опытом работы в сфере ИТ.

Ключевые вопросы, которые следует рассмотреть, включают:

какова стоимость внешней оценки риска по сравнению с одним киберинцидентом?

что моя доска сделала, чтобы эффективно продемонстрировать, что она решает эту проблему?

Знаю ли я об ИТ и киберрисках в той же степени, что и о стратегии, операциях и кадрах?

Вероятно, что у большинства фирм нет адекватных ответов на некоторые из этих вопросов. Распространенной ошибкой является предположение, что оперативная оперативность, которую мы наблюдали за последний год при переходе к удаленной работе, автоматически означает способность победить киберпреступников. Это не одни и те же угрозы. Хотя многие опытные лидеры приобрели новые навыки, знания и уверенность в технологиях за последний год, это не заменит правильного выявления, измерения и защиты от киберугроз.

Организации, которые сейчас инвестируют в обучение, системы и внешние оценки, имеют шанс столкнуться с кибератакой.

На уровне правления необходимо признать, что создание культуры осведомленности о рисках, развитие навыков, способность проверять и наличие правильного руководства для реагирования - это долгосрочная игра.

Противодействие киберпреступности - разработка плана реагирования на стихийные бедствия

Фирмы должны подумать о том, что они могут сделать, чтобы ограничить ущерб после кибератаки или кибербезопасности. Две важные меры включают наличие четкого плана реагирования на стихийные бедствия и полиса киберстрахования, адаптированного к конкретным потребностям бизнеса, обеспечивающего комплексное покрытие конкретных киберрисков и связанных с ними убытков.

План реагирования на стихийные бедствия должен быть адаптирован к основным угрозам, исходящим от каждого бизнес-подразделения, и четко определять, что следует делать в случае кибератаки. План должен регулярно обновляться, что означает включение в него самых основных задач, таких как обеспечение актуальности контактных данных. ИТ-специалисты необходимы для решения технической стороны киберзащиты. Однако для того, чтобы у фирмы был надежный план защиты и реагирования на стихийные бедствия, этот вопрос должен рассматриваться на уровне совета директоров, где есть полное понимание бизнеса и оценка воздействия кибератаки.

Когда происходит кибератака, жертве необходимо очень быстро отреагировать и привлечь эксперта по кибербезопасности для расследования инцидента. Юридическая консультация также нужна в срочном порядке. Юристы принимают активное участие в некоторых из первых важных шагов, включая оказание помощи в подаче жалобы в прокуратуру, специализированные полицейские подразделения и подразделение финансовой разведки, а также управление коммуникациями и сотрудничество с этими государственными органами. Юридическая помощь также обычно требуется для обеспечения эффективного взаимодействия с банками и увеличения шансов на возвращение украденных средств.

Во многих случаях ИТ-система была взломана обманным путем, и мошенник сделал банковский перевод. Возможна отмена заказа при своевременном обращении в банк. Кроме того, органы прокуратуры могут повторно отслеживать

банковские переводы и получать приказы о замораживании счетов через сотрудничество с иностранными властями.

Чем быстрее будут предприняты действия, тем успешнее будут усилия.

Это работает для блокировки средств, прежде чем они могут быть переведены на другие банковские счета по всему миру. Быстрая, хорошо организованная и скоординированная реакция на кибератаку необходима для максимального увеличения шансов на возвращение средств, присвоенных мошенническим путем.

В контексте Общего регламента по защите данных (GDPR) юридическая консультация также необходима для возможного сообщения Национальной комиссии по защите данных (Управление по защите данных) о том, что в ходе кибератаки произошла утечка личных данных.

Бесспорно, что киберпреступность стала более распространенной и более разрушительной для предприятий любого размера. Важно, чтобы каждый бизнес принимал все превентивные меры для защиты и имел план реагирования (который был отрепетирован), который был бы готов к выполнению, как только произойдет атака. Принимая эти стратегии, компании лучше всего могут быстро реагировать и минимизировать потенциальный финансовый и репутационный ущерб». ***(Michael Schweiger. Cyber attacks: getting prepared and responding effectively // Loyens & Loeff (https://www.loyensloeff.com/en/en/news/news-articles/cyber-attacks-getting-prepared-and-responding-effectively-n22341/). 22.04.2021).***

***

«Угрозы киберпреступности существуют, по крайней мере в примитивных формах, примерно с 1970-х годов, примерно в то время, когда первые коммерческие технологии ЛВС (количество соединенных вместе устройств является локальной сетью) экспериментировались и развивались. Это также как раз в то время, когда Интернет родился как ARPANET, который иногда называют дедушкой Интернета. Рождение первого " компьютер-компьютер"«Связи должны были соответствовать зарождению киберпреступности и появлению того, что позже будет названо «киберпреступниками». Хороший способ сравнить это с реальной жизнью - это то, что, как только торговля между цивилизациями стала развиваться, возникли и группы воров, которыми, по сути, и является большинство киберпреступников. Первым «червем» (компьютерным вирусом или вредоносной программой) был червь Морриса в 1988 году, который в то время заразил систему UNIX Noun 1 и воспроизвел себя, что сделало компьютеры в сети непригодными для использования. Создатель червя Роберт Тапан Моррис был первым человеком, который был осужден по закону за киберпреступность в США. Он сказал, что пытался измерить размер Интернета с помощью этой техники. Киберпреступность сейчас свирепствует каждую секунду и повсюду в самых разных формах,

Генеральный директор IBM подтвердил самое большое количество людей: «Киберпреступность - самая большая угроза для каждой компании в мире». Официально ущерб от киберпреступности оценивается в 6 триллионов долларов

ежегодно, не говоря уже о повреждении человеческого компонента, и это число будет расти.

Сегодня в 2021 году киберпреступность и ее последствия возрастут. Возникающие угрозы кибербезопасности и способы подготовки к ним стратегий кибербезопасности - одни из самых значительных дискуссий не только в ИТ-кругах, но и в мировой экономике. Угрозы адаптируются и изменяются с беспрецедентной скоростью, в то время как группы защиты кибербезопасности и регулирующие органы борются с постоянным давлением этих кибератак. Согласно исследованию Gartner, «две главные проблемы, которые беспокоят корпоративные советы директоров» - это кибербезопасность и соответствие нормативным требованиям. Кроме того, «С увеличением количества нарушений общественной безопасности и усложняющимися настройками безопасности советы директоров уделяют больше внимания кибербезопасности». Кибербезопасность - это огромная проблема, подтвержденная тем фактом, что Всемирный экономический форум (ВЭФ) сказал следующее в своем отчете «Кибербезопасность как одна из наиболее стратегически важных проблем в мире.

Прежде чем углубляться в экстренные угрозы кибербезопасности, важно определить, как киберпреступники выстраивают стратегию своих атак через различные «каналы доставки».

Поверхность атаки киберпреступности

Поверхность атаки киберпреступника в некотором смысле не требует пояснений, поскольку она буквально определяет поверхность, доступную злоумышленнику (кибер-злоумышленнику) для совершения киберпреступлений. Поверхность атаки может варьироваться от аппаратных и программных поверхностей, уязвимых для атак киберпреступников. Поверхности атаки могут варьироваться от любого устройства, подключенного к Интернету, которое является аппаратным компонентом (устройствами), до цифровых конечных точек (программного обеспечения) в цепочке.

Векторы атак киберпреступности

Вектор атаки - это метод, которым киберпреступники нацеливаются на цифровое или физическое устройство на поверхности атаки (определено выше). Например, червь или вирус как вектор атаки. Более подробное объяснение может заключаться в том, что вектор атаки может варьироваться от следующих методов; фишинг, вредоносное ПО, взломы методом перебора, программы-вымогатели и многое другое.

Типы киберугроз сегодня

Сегодня горизонт киберугроз совсем другой, чем он был в 2010-х годах, не говоря уже о том, что раньше, когда киберпреступность была далека от нынешних масштабов. В 2021 году главный отличительный фактор - это то, что земной шар находится под ограничениями. Эти ограничения навсегда изменили сферу кибербезопасности, потому что вся экономика зависит от удаленной работы и моделей общения и ведения бизнеса WFH (Работа из дома). В отдаленном обществе круг наиболее распространенных киберугроз выглядит следующим образом;

Утечки данных будут возникать из-за халатного отношения сотрудников к личным устройствам.

Значительное внедрение ИИ во всем мире находится под угрозой из-за отсутствия стратегий безопасности

5G усугубит угрозы для систем управления производством

Число атак национальных государств, геополитически мотивированных групповыми атаками APT, растет

Атаки социальной инженерии, такие как фишинг, составляют 90% успешных кибератак, а целевой фишинг - еще хуже.

Атаки программ-вымогателей и вредоносных программ останутся проблемой

Каковы новые угрозы кибербезопасности?

Остальная часть этого десятилетия будет отмечена переходом к искусственному интеллекту, машинному обучению., Сети 5G, все больше и больше полагаться на облачные вычисления, увеличивающееся количество устройств Интернета вещей и внедрение интеллектуальных датчиков. Этот список принесет бесконечную головную боль индустрии кибербезопасности, если в отрасли не будут реализованы чрезвычайно строгие и строгие политики сдерживания. В этом десятилетии ожидается дальнейшая цифровая трансформация, и в экономику будет внедряться все больше и больше «нечеловеческих сущностей», а это означает, что управление идентификацией машин жизненно важно для стратегии кибербезопасности. После этого настойчивое требование отрасли к 5G, облачным вычислениям и интеллектуальным датчикам потребует множества политик и инструментов, поскольку все это значительно расширяет поверхность атаки (что позволяет расширить каналы доставки) и упростит пути проникновения векторов атак. через систему.

Наконец, индустрия Интернета вещей или Интернета вещей будет только продолжать расти и продавать миллиарды устройств, которые увеличивают глобальный ландшафт угроз кибербезопасности. Неопределенные методы ведения бизнеса, недостаточные стратегии кибербезопасности и особенно отсутствие специализированного обучения сотрудников по вопросам кибербезопасности станут слабыми сторонами в этом десятилетии. Включение сценариев BAS (моделирование взлома и атаки) в каждый бизнес поможет смягчить множество проблем, а также PEC (вычисление повышения конфиденциальности). Оптимизация безопасностибизнес-процессов и потоков, которые сейчас более уязвимы, чем когда-либо, также является важной обязанностью кибербезопасности. Наконец, подготовка и стратегия кибербезопасности на будущее означает понимание того, что антивирусное программное обеспечение, простые резервные копии файлов и пароли больше не помогут в этом возникающем, постоянно меняющемся ландшафте угроз.

Почему так сложно остановить киберпреступность?

Вокруг киберпреступности столько ажиотажа, что можно задаться вопросом, как во втором десятилетии 21 века, когда человечество разрабатывает системы искусственного интеллекта и даже квантовые компьютеры, индустрия неспособна бороться с киберпреступниками и их методами. Проще говоря, это связано с тем, что не хватает хорошо обученного персонала по кибербезопасности, а также

потому, что вредоносное ПО развивается и адаптируется. Персонал, занимающийся обнаружением угроз, не может достаточно быстро реагировать на огромное количество предупреждений системы безопасности в сочетании с нехваткой навыков кибербезопасности. Давайте возьмем в качестве примера самую ужасную и изощренную кибератаку в истории - недавнюю атаку SolarWinds прошлой весной. Генеральный директор компании сказал следующее: «Из-за узкого окна, в котором вредоносная программа была внедрена в код, способность наших систем сборки идентифицировать то, что не существовало. Это одна из ключевых областей, над которой мы работаем», «Эта проблема существует в каждой компании, поэтому то, что случилось с нами, может случиться с любым разработчиком программного обеспечения в мире». ***(Emerging Cybersecurity Threats in 2021 // St Louis News.Net - Mainstream Media Ltd (https://www.stlouisnews.net/news/269073769/emerging-cybersecurity-threats-in-2021). 29.04.2021).***

***

«Поставщик технологий говорит, что атака вредоносного ПО вызвала отключение на несколько дней, что привело к сбою систем бронирования примерно у 20 бюджетных авиакомпаний по всему миру.

Компания Radixx заявила, что во вторник заметила «необычную активность» вокруг своей программы бронирования. В нем не описывалось вредоносное ПО и не говорилось, как оно попало в программу.

Пресс-секретарь материнской компании Radixx, Саутлейк, штат Техас, Sabre Corp., заявила в пятницу, что компания начинает восстанавливать обслуживание клиентов авиакомпаний. Кристин Хейс сказала, что компания сообщила об инциденте в ФБР.

Radixx заявила, что ее система работает отдельно от систем, используемых некоторыми крупными авиакомпаниями, которые являются клиентами Sabre. Radixx заявила, что информация о клиентах не была скомпрометирована.

Сроки вряд ли могут быть хуже для начинающей авиакомпании Avelo Airlines, которая не может обрабатывать бронирования, поскольку она готовится к своему первому полету на следующей неделе в Калифорнии. На своей домашней странице Avelo извинился перед клиентами и призвал их просматривать списки рейсов, даже если они не могут забронировать поездку.

Южноафриканская бюджетная авиакомпания FlySafair заявила, что создала «мини-платформу бронирования», которая позволяет клиентам покупать билеты в один конец на рейсы до следующего вторника.

«Мы не уверены, когда мы снова поднимемся», - говорится в сообщении авиакомпании на своем веб-сайте.

Vietravel Airlines, новый перевозчик во Вьетнаме, заявила, что проводит техническое обслуживание системы, но все еще продает билеты на стойках аэропорта.

Регулярно происходят сбои в технологических системах авиакомпаний, что затрудняет выполнение рейсов и делает невозможным бронирование для клиентов.

Только в США аудиторы Конгресса насчитали примерно одно отключение в месяц с 2015 по 2017 год.

Эксперты говорят, что это отчасти потому, что системы часто состоят из слоев старых и новых технологий, которые не всегда идеально работают вместе». ***(Outages Blamed on Malware Still Plaguing Budget Airlines // Wired Business Media (https://www.securityweek.com/outages-blamed-malware-still-plaguing-budget-airlines). 26.04.2021).***

***

«Управление полиции Вашингтона, округ Колумбия, заявило в понедельник, что его компьютерная сеть была взломана, а русскоязычный синдикат вымогателей утверждал, что украл конфиденциальные данные, в том числе об осведомителях, которые он пригрозил передать местным преступным группировкам, если полиция не заплатит неуказанный выкуп.

Киберпреступники разместили на своем темном веб-сайте скриншоты, подтверждающие их утверждение о краже более 250 гигабайт данных.

Столичное управление полиции округа Колумбия заявило в своем заявлении, что оно попросило ФБР расследовать «несанкционированный доступ». Не было никаких указаний на то, что какие-либо операции полиции были затронуты, и департамент не сразу сказал, была ли поражена программа-вымогатель.

Группа Бабук, относительно новая банда вымогателей, заявила на своем веб-сайте, что «загрузила достаточный объем информации из ваших внутренних сетей» и дала полиции три дня на то, чтобы связаться с ней, или «мы начнем связываться с бандами, чтобы слить воду. информаторы».

Скриншоты, которые он опубликовал, предполагают, что у него есть данные как минимум с четырех компьютеров, включая отчеты разведки, информацию о конфликтах между бандами, перепись в тюрьмах и другие административные файлы. На одном из изображений, очевидно, сетевых местоположений, к которым имели доступ преступники, был показан текстовый документ на одном компьютере под названием «Как восстановить ваши файлы».

Такие документы обычно включают инструкции о том, как связаться с преступниками-вымогателями, стандартная рабочая процедура которых заключается в эксфильтрации конфиденциальных данных из сетей, в которые они проникают, когда они сеют вредоносное ПО, которое после активации шифрует данные. Только после получения оплаты злоумышленники предоставляют программные ключи, которые расшифровывают данные.

По словам аналитика по программам-вымогателям Бретта Кэллоу из компании Emsisoft, аналитика по программам-вымогателям на данный момент в этом году 26 государственных учреждений в США были поражены программами-вымогателями, при этом киберпреступники публикуют онлайн-данные, украденные у 16 из них. Жертвы программ-вымогателей не всегда платят, часто предпочитая сложную задачу восстановления сетей из резервных копий.

В полицейском управлении округа Колумбия заявили, что серьезно относятся к угрозе.

«Нам известно о несанкционированном доступе к нашему серверу. В то время как мы определяем полное воздействие и продолжаем анализировать деятельность, мы привлекли ФБР для полного расследования этого дела», - говорится в заявлении департамента. Представитель ФБР не дал никаких комментариев.

Усиливающаяся глобальная эпидемия атак программ- вымогателей многими рассматривается как угроза национальной безопасности и наносит ущерб в десятки миллиардов долларов. Правоохранительные органы США относительно бессильны противодействовать этому, поскольку большинство преступников пользуются убежищем в России и других странах со слабым верховенством закона». ***(DC Police Department Hit by Apparent Extortion Attack // Wired Business Media (https://www.securityweek.com/dc-police-department-hit-apparent-extortion-attack). 27.04.2021).***

***

«Ожидание, связанное с предстоящей в воскресенье трансляцией 93-й церемонии вручения премии Оскар, используется мошенниками, чтобы обманом заставить людей отказаться от своих полномочий - они думают, что собираются транслировать фильмы, номинированные на Оскар, но на самом деле все обстоит иначе.

До объявления победителей во время церемонии многие любители кино хотят посмотреть как можно больше номинированных фильмов. Мошенники это знают и готовы нанести удар.

«В надежде посмотреть фильм, номинированный на «Оскар», пользователи посетили сайт, где им показали первые несколько минут фильма, прежде чем их попросили зарегистрироваться для продолжения просмотра», - подробно говорится в отчете «Лаборатории Касперского», опубликованном в пятницу. «При регистрации для подтверждения региона проживания потерпевшего попросили ввести данные своей банковской карты. Через некоторое время с карты были списаны деньги, и, как и ожидалось, фильм не продолжался».

Названия из фильма "Лучший фильм" Оскара Категории, о которых больше всего ругают

Фильмы также используются для распространения вредоносных программ. За последний год группа исследователей «Лаборатории Касперского» выявила около 80 вредоносных файлов, связанных с фильмами, номинированными на премию «Оскар» «Лучший фильм». Из них 70 процентов распространились по ссылкам, чтобы якобы посмотреть один из трех фильмов: «Иуда и Черный Мессия» (фильм, о котором больше всего ругают, на его долю приходится 27 процентов вредоносных программ); Многообещающая молодая женщина - 22 процента; и «Суд над Чикаго-7», который был связан с 21 процентом файлов, подвергшихся злоупотреблениям.

Касперский обнаружил, что другие номинированные на премию Оскар фильмы, используемые для распространения вредоносных программ, включают Nomadland (14 процентов), Mank (6 процентов), Minari (5 процентов), The Father (3 процента) и Sound of Metal (3 процента).

Аналитики добавили, что этот тип атак является обычным явлением, но проблемы с безопасностью немного ослабевают благодаря росту потоковых сервисов и повышению безопасности видеоконтента.

«Киберпреступники всегда пытались монетизировать интерес пользователей к различным источникам развлечений, включая фильмы, - сказал Антон Иванов, эксперт по безопасности Kaspersky. «Мы видим, что крупные события в киноиндустрии могут повысить интерес киберпреступников, но сегодня этот вид вредоносной деятельности не так популярен, как раньше. В настоящее время все больше и больше людей переходят на потоковые сервисы, которые более безопасны, поскольку не требуют загрузки файлов. Тем не менее, фильмы служат популярной приманкой для распространения фишинговых страниц и спама по электронной почте».

Глобальные заголовки приносят хорошие деньги мошенникам

Практически любое всемирное событие, вызывающее заголовки, - это возможность для киберпреступников нажиться. Все, от праздников, таких как День святого Валентина, до глобальных спортивных событий, таких как чемпионат мира по футболу FIFA, является потенциальной приманкой для жертв, желающих погрузиться в безумие.

Лучшая защита от таких видов мошенничества - это научить пользователей вообще не переходить по этим вредоносным ссылкам.

«Обучение сотрудников тому, как распознавать подобные фишинговые электронные письма, так же важно, как и установка систем защиты», - сказала Threatpost Хизер Паунет, старший вице-президент Untangle. «По мере того, как злоумышленники находят новые творческие способы проникновения в сети, постоянное обучение сотрудников и их обновление необходимо для усиления сетевой безопасности». ***(Becky Bracken. Oscar-Bait, Literally: Hackers Abuse Nominated Films for Phishing, Malware // Threatpost (https://threatpost.com/oscar-bait-hackers-nominated-phishing-malware/165583/). 23.04.2021).***

***

«Любой, кто пользуется смартфоном, скорее всего, стал целью как минимум одной атаки с уничтожением. Smishing очень похож на фишинговую рассылку электронной почты, но вместо этого отправляет вводящие в заблуждение или вредоносные ссылки через текстовые сообщения.

Подобно фишингу, smishing пытается обманом заставить пользователей отказаться от ценной информации, такой как учетные данные для входа в банк, убеждая получателя в том, что сообщение пришло из надежного источника. Хотя эти типы мошенничества используют учетные записи электронной почты на протяжении десятилетий, профессионалов в области кибербезопасности следует особенно беспокоить из-за резкого увеличения количества атак smishing за последние пару лет.

Еще до того, как эра COVID-19 вынудила организации переключиться на удаленную работу почти в одночасье, примерно 81 процент организаций заявили, что их сотрудники испытали сокрушительную атаку на свои мобильные устройства. В 2020 году, после того как по всему миру были введены блокировки,

сокрушительные атаки участились в геометрической прогрессии. Одно исследование показало, что с марта по июль 2020 года количество этих атак увеличилось на тревожные 29 процентов.

Почему сейчас люди более уязвимы перед улыбкой?

Хотя фишинговые атаки существуют вечно, есть по крайней мере несколько причин, по которым smishing является более опасным для ИТ-безопасности сегодня:

Гораздо проще заблокировать фишинг электронной почты на корпоративных ПК, но сегодняшние удаленные сотрудники теперь используют свои личные устройства для доступа к корпоративным приложениям и данным. И, честно говоря, просто нет простого способа проверить подлинность URL-адресов на смартфонах, поэтому пользователи часто просто щелкают и надеются на лучшее.

По состоянию на 2020 год 2,8 миллиарда пользователей по всему миру носят смартфоны. Устройства буквально повсюду, обеспечивая хакерам обширный, пригодный для использования ландшафт угроз.

Мобильные пользователи обычно открывают текстовые сообщения и отвечают на них гораздо чаще, чем на электронную почту. Учтите, что 90 процентов текстовых сообщений открываются и читаются практически сразу; Между тем, средний показатель открытия электронной почты составляет около 20 процентов.

Персональным устройствам обычно не хватает надежной защиты, используемой для защиты корпоративных устройств.

Посмотрим правде в глаза, слишком часто мы просто не обращаем внимания. Многие ли из нас проверяют свои телефоны, когда занимаются другими делами, такими как покупки, едят, смотрят фильмы или гуляют с собакой?

И угадай что? Все это знают и хакеры. С помощью небольшого исследования и настойчивости они могут легко обманом заставить сотрудника раскрыть свои корпоративные данные. Попав внутрь компании, хакеры могут быстро развязать кошмар безопасности для любой ИТ-организации. Помните взлом Твиттера в июле прошлого года?

Поскольку новая эра массовой удаленной работы в значительной степени разрушила то, что осталось от традиционного периметра сети, директорам по информационной безопасности необходимы новые стратегии защиты корпоративных приложений и данных, где бы они ни находились, в любой сети, устройстве или облаке. Хорошая новость заключается в том, что большинство руководителей по информационной безопасности, похоже, понимают, что защита своих организаций от мобильных угроз должна стать их важнейшим приоритетом в будущем.

Список дел по безопасности мобильных устройств CISO

В декабре 2020 года моя компания Ivanti заказала у Vanson Bourne независимое исследование, чтобы лучше понять приоритеты CISO. Выяснилось, что 87% директоров по информационной безопасности в странах Европы, Ближнего Востока и Африки заявили, что безопасность мобильных устройств теперь является основным направлением их стратегий кибербезопасности. Почти 80 процентов этих руководителей по информационной безопасности знают, что

пароли больше не являются эффективным или безопасным средством аутентификации пользователей, и почти две трети (64 процента) считают, что в 2021 году одним из основных приоритетов будет инвестирование в программное обеспечение для обнаружения мобильных угроз.

Пользовательский опыт имеет важное значение для мобильной безопасности

Конечно, ни один подход к безопасности мобильных устройств не может быть успешным, если он не улучшает пользовательский опыт. Это еще более важно сегодня, когда так много сотрудников работают удаленно, возможно, на постоянной основе.

Отказ от паролей в пользу многофакторной аутентификации (MFA) - одна из самых простых вещей, которые сейчас могут сделать руководители по информационным технологиям, чтобы помочь удаленным сотрудникам оставаться продуктивными и минимизировать угрозы безопасности. Требуя биометрии или других факторов для аутентификации, ИТ-отдел может снизить «фишабильность» учетных данных имени пользователя и пароля, которые невероятно легко украсть с помощью относительно простых средств. Не менее важно, что MFA значительно улучшает взаимодействие с пользователем, устраняя необходимость вводить сложные и легко забываемые пароли на маленьких экранах.

Хотя упрощенная аутентификация пользователей является необходимым шагом, автоматизация подходов к безопасности мобильных устройств является неотъемлемой частью любой стратегии безопасности мобильных устройств. Директора по информационной безопасности знают, что они не могут просто полагаться на людей, склонных к ошибкам и отвлекающих внимание, для предотвращения киберпреступников. Комплексный и постоянно действующий подход к мобильной безопасности (доступный у большинства поставщиков кибербезопасности), который может обнаруживать и предотвращать мобильные угрозы, не влияя на доступ сотрудников, должен быть во главе списка дел каждого директора по информационной безопасности в предстоящем году». ***(Phil Richards. Smishing: Why Text-Based Phishing Should Be on Every CISO's Radar // Threatpost (https://threatpost.com/smishing-text-phishing-ciso-radar/165634/). 27.04.2021).***

***

«Злоумышленники выдают себя за Chase Bank в двух фишинговых атаках, которые могут обойти средства защиты Microsoft Exchange с целью кражи учетных данных жертв - путем имитации реальных сценариев клиентов.

Исследователи из Armorblox недавно обнаружили атаки, одна из которых утверждает, содержат выписки по кредитной карте, в то время как другие пользователям сообщает, что их он-лайн доступ к учетной записи был ограничен из - за необычную активность входа в системе, в соответствии с постом на Armorblox блоге опубликовал вторник.

Первый набор электронных писем был разослан в 9000 почтовых ящиков в среде клиента Armorblox, а второй - до 8000, написал в своем посте Прит Кумар, старший менеджер по работе с клиентами в Armorblox.

По ее словам, обеим атакам удалось обойти две защиты Microsoft Exchange - Exchange Online Protection (EOP) и Microsoft Defender для Office 365 (MSDO) - на пути к почтовым ящикам клиентов.

«В этих атаках на электронную почту использовался целый ряд методов, позволяющих обойти традиционные фильтры безопасности электронной почты и пройти проверку зрения ничего не подозревающих конечных пользователей», - написал Кумар.

Согласно отчету, в первом сценарии злоумышленники отправили электронное письмо с заголовком «Выписка по вашей кредитной карте» с именем отправителя «JP Morgan Chase» со стилем HTML, аналогичным подлинным электронным письмам, отправленным от Chase. В электронном письме были ссылки, по которым жертва могла просмотреть свое заявление и произвести платежи.

«Microsoft присвоила письму уровень вероятности нежелательной почты (SCL) «-1», что означало, что оно пропустило фильтрацию спама, поскольку Microsoft определила, что письмо было отправлено от надежного отправителя, надежному получателю или было отправлено с исходного сервера электронной почты на список разрешенных IP-адресов», - написал Кумар в отчете.

По ее словам, ссылки ведут потенциальных жертв на фишинговую страницу, которая напоминает портал входа в Chase и запрашивает учетные данные их банковских счетов. Исследователи предположили, что URL-адрес страницы, скорее всего, был приобретен и размещен с помощью NameSilo, который предоставляет клиентам услуги хостинга, электронной почты и SSL.

«Подобные услуги полезны для миллионов людей во всем мире, но, к сожалению, также снижают планку для киберпреступников, стремящихся запустить успешные фишинговые атаки», - заметил Кумар.

Мошенничество в сфере обслуживания клиентов Chase

Другая фишинговая атака начинается с электронного письма, озаглавленного «СРОЧНО: необычная активность при входе», в котором утверждается, что отправителем была «служба поддержки клиентов банка Chase Bank», - сказал Кумар.

В электронном письме была ссылка, по которой клиенты должны были подтвердить свою учетную запись для восстановления доступа, и использовалась обычная тактика мошенников, заключающаяся в использовании разных адресов «от» и «для ответа».

Как и в случае с другим электронным письмом, нажатие на ссылку приведет к фишинг-странице, на которой пользователи будут пытаться ввести свои учетные данные, согласно сообщению. Однако в этом случае страница уже была неактивной к тому времени, когда исследователи исследовали кампанию, заявили они.

Письмо с подтверждением учетной записи также не было обнаружено Exchange и было признано безопасным с оценкой «1» по уровню достоверности спама, отметил Кумар.

Как обнаружить фишинговые письма

Однако есть некоторые явные признаки того, что оба письма вызывают подозрение, если получатели таких сообщений знают, на что обращать внимание, говорят исследователи, излагая их в сообщении.

Они включают вышеупомянутое использование разных адресов «для ответа» и «от»; использование страницы, которая выглядит так, как будто она принадлежит Chase, но с URL-адресом, не совпадающим с названием веб-сайта компании; и тема безопасности, которая требует, чтобы кто-то ввел личные данные безопасности, предприняв второстепенные действия.

«Поскольку мы получаем так много электронных писем от поставщиков услуг, наш мозг обучен быстро выполнять запрошенные ими действия», - написал Кумар. «Гораздо легче сказать, чем сделать, но используйте эти электронные письма рационально и методично, когда это возможно».

Атаки - это не первый случай, когда клиенты Chase подвергаются фишинговым атакам, и, вероятно, не последний. Этот банк был одним из нескольких, включая Royal Bank of Canada и TD Bank, на которые в феврале 2020 года была распространена SMS-фишинговая кампания, в которой использовались поддельные текстовые сообщения безопасности для нацеливания на пользователей приложений онлайн-банкинга». ***(Elizabeth Montalbano. Chase Bank Phish Swims Past Exchange Email Protections // Threatpost (https://threatpost.com/chase-bank-phish-sexchange-email-protections/165653/). 28.04.2021).***

***

«Фишинговая кампания, обнаруженная исследователями из Cofense, оборачивается темой Microsoft Office SharePoint и успешно обходит защитные шлюзы электронной почты (SEG). В сообщении во вторник компания заявила, что это пример того, почему не всегда разумно обмениваться документами через чрезвычайно популярную и широко используемую платформу для совместной работы Microsoft SharePoint.

Фишинг нацелен на пользователей Office 365 с легитимным на вид документом SharePoint, в котором утверждается, что срочно нужна подпись электронной почты. Кампания возникла в месте, которое должно было быть защищено собственной SEG Microsoft. Это не первый раз, когда мы видим, как святилище SEG загрязняется: в декабре копейщики подделали сам Microsoft.com, чтобы нацелить 200 миллионов пользователей Office 365, успешно ускользнув от контроля SEG из-за того, что Microsoft сообщила о неспособности обеспечить соблюдение доменов на основе аутентификации сообщений, отчетности и соответствия (DMARC): протокол аутентификации электронной почты, созданный специально для предотвращения точного спуфинга домена (SPF / DKIM).

«Срочно ответить…?»

Как видно из этого изображения текста в фишинговом письме, орфография и грамматика, использованные в заминированном сообщении, не являются самыми вопиющими, ужасно написанными, синтаксически причудливыми подарками, которые вы можете найти в подобных фишинговых кампаниях. Но опять же, можно с уверенностью предположить, что любое сообщение SharePoint с просьбой «срочно ответить» исходит не от носителя языка.

Сам факт того, что сообщение требует от получателей срочности, конечно, должен быть наводкой: «Спешка» - это типичный фишинговый ход. Cofense отмечает, что другие красные флажки включают тот факт, что имя пользователя не отображается в начальном сообщении: это признак того, что это кампания массового распространения, предназначенная для достижения многих целей.

Кроме того, когда получатели наводят курсор на гиперссылку, они не видят никаких ссылок на Microsoft. Те, кто нажимает на ссылку, вместо этого будут перетасованы на целевую страницу, показанную ниже, на которой отображается логотип Microsoft SharePoint и уведомление «Ожидающий файл» на размытом фоне и запрос предполагаемой жертве войти в систему для просмотра документа. По словам Кофенс, этого «злоумышленникам может хватить для извлечения и сбора личных данных пользователей». Если и когда учетные данные переданы, кампания перенаправляет пользователя к поддельному несвязанному документу, «которого может быть достаточно, чтобы заставить пользователя думать, что это законная транзакция», - говорит Кофенс.

В своем отчете X-Force Threat Activity Report IBM назвала фишинг угрозой с высоким риском и дала следующие рекомендации:

Убедитесь, что антивирусное программное обеспечение и связанные файлы обновлены.

Найдите существующие признаки указанных инцидентов взлома (IoC) в вашей среде.

Рассмотрите возможность блокировки и / или настройки обнаружения для всех IoC на основе URL и IP.

Поддерживайте работу приложений и операционных систем на уровне текущего выпущенного исправления.

Будьте осторожны с вложениями и ссылками в электронных письмах.

Несмотря на высокий риск, эта фишинговая кампания в основном представляет собой еще одну историю о злоумышленнике, размещающем поддельный материал, который выглядит законным, с целью побудить пользователей щелкнуть мышью в надежде получить учетные данные. Не пожмет его, хотя: это еще одна атака на серверы SharePoint, которые теперь присоединились к реестру сетевых устройств - в том числе много-запутаны почтовых серверов Microsoft Exchange, SonicWall шлюзы и импульсно Безопасные шлюзы - которые в настоящее время используются вымогателей банд чтобы воспрепятствовать открытым корпоративным сетям.

Это подводит нас к программе-вымогателю: вторая пощечина в двойном ударе по SharePoint:

Банда программ-вымогателей пингует боль через Wickr

Это довольно новый вариант, впервые замеченный Пондурансом в январе. Аналитики называют это двумя именами: Hello, поскольку в некоторых образцах.hello используется в качестве расширения; или WickrMe, поскольку банда, которая его продвигает, использует зашифрованную службу обмена мгновенными сообщениями Wickr, чтобы попытаться избавиться от жертв с целью получения выкупа.

Злоумышленники используют пыльную уязвимость Microsoft SharePoint 2019 (CVE-2019-0604), чтобы проникнуть в сети жертв. Оттуда они используют Cobalt Strike, чтобы перейти к контроллеру домена и запустить атаки программ-вымогателей.

CVE-2019-0604 - это уязвимость CVE с высоким уровнем серьезности, которая может привести к удаленному выполнению кода. Microsoft исправила этот недостаток в марте 2019 года, но, тем не менее, похоже, что с тех пор атакам, которые использовали его для проникновения на незащищенные серверы, нет конца. Один из примеров: в октябре 2020 года Microsoft предупредила, что иранские субъекты национального государства используют CVE-2019-0604 для эксплуатации удаленных серверов без исправлений, а затем для имплантации веб-оболочки для получения постоянного доступа и выполнения кода. После установки веб-оболочки злоумышленник развертывает Cobalt Strike - коммерчески доступный инструмент для тестирования на проникновение, который они позже используют для установки бэкдора, который позволяет им запускать автоматический сценарий PowerShell, который в конечном итоге загружает и устанавливает окончательную полезную нагрузку: программу-вымогатель Hello / Wickr.

Джефф Костлоу, директор по информационной безопасности ExtraHop, сообщил Threatpost в среду, что атаки программ-вымогателей на уязвимость 2019 года, затрагивающую серверы SharePoint, представляют собой более коварную угрозу в двойном ударе, поскольку они устанавливают программное обеспечение для удаленного управления и, таким образом, предоставляют прямой доступ к инфраструктуре, где злоумышленники могут свободно порезвиться.

«Общей нитью является сервер SharePoint», - сказал Костлоу в электронном письме. «Любой, кто использует SharePoint, должен убедиться, что он исправляет любые экземпляры SharePoint, чтобы избежать установки вредоносных программ / программ-вымогателей. В долгосрочной перспективе, никакие исправления не решат проблему фишинга. Злоумышленникам слишком легко создавать сайты, имитирующие легитимные сайты. Нам нужно переосмыслить, как осуществляется совместное использование. Команды безопасности должны занять проактивную позицию, чтобы помочь своим пользователям вести бизнес безопасно. Существуют различные тактики, помогающие предупреждать пользователей о возможных атаках, например, настройка каждого сервера SharePoint для использования знакомого фона или изображения, чтобы пользователи могли вводить учетные данные только на легитимных сайтах».

Два отдельных укола SharePoint

Cofense сообщил Threatpost в электронном письме в среду утром, что нет очевидной связи между фишинговой кампанией SharePoint, которую раскрыли ее аналитики, и продолжающейся эксплуатацией уязвимостей сервера SharePoint группой программ-вымогателей Wickr / Hello.

Но один эксперт заметил, что в схеме, которой следуют эти атаки, существует монотонная закономерность: сначала мы получаем новости об уязвимости, затем на нее набрасываются злоумышленники, ищущие незакрепленных серверов.

В электронном письме Threatpost в среду Авихай Бен-Йосеф, технический директор и соучредитель Cymulate, сказал, что мы видели, как это происходит снова и снова. «В последний год мы наблюдаем повторяющуюся картину подобных атак. «Нулевой день» используется субъектом национального государства», - сказал он. «Затронутая компания - в данном случае Microsoft - объявляет об уязвимости и впоследствии исправляет ее. Затем другие субъекты национального государства, узнав об уязвимости, впоследствии начинают атаки на тех, кто не установил исправления. Наконец, приходят злоумышленники-вымогатели, социализируют эксплойт на сайтах Dark Net и используют его... для запуска собственных атак. Двойной удар по SharePoint заключается в том, что субъекты национального государства использовали его сначала как нулевой день (а затем как известную уязвимость). Затем пришли злоумышленники и тоже использовали его.

«Идея состоит в том, чтобы знать, какие у вас проблемы и где», - сказал он. «Если вы не знаете, вы не сможете защитить себя. Организации должны разработать более эффективные возможности реагирования, чтобы быстрее отслеживать эти объявления, анализ угроз и исправлять их». ***(Lisa Vaas. Microsoft Office SharePoint Targeted With High-Risk Phish, Ransomware Attacks // Threatpost (https://threatpost.com/sharepoint-phish-ransomware-attacks/165671/). 28.04.2021).***

***

«После приписывания атаки цепочки поставок SolarWinds российской APT29, американское информационное агентство CISA опубликовало список известных тактик шпионов, включая склонность к использованию провайдера электронной почты с озорным именем.

APT29 * - это кодовое название в западном мире информационной безопасности того, что, как мы теперь знаем, - это Служба внешней разведки России, известная под ее русской аббревиатурой SVR.

Помимо публикации списка того, что контрразведка США знает о своих российских наступательных коллегах, CISA также добавила несколько советов о том, как избежать этой общей тактики компромисса российской разведки.

Профессионалы взлома SVR используют такие методы, как «низкое и медленное» распыление паролей, нацеленных на известные учетные записи администраторов, развертывание нулевого дня на устройствах VPN, а затем развертывание дропперов, таких как WellMess.

Первоначальные результаты ФБР указывают на то, что постинфекционная торговля похожа на другие вторжения, спонсируемые SVR, в том числе на то, как субъекты приобретали и управляли инфраструктурой, использованной во вторжениях. Получив доступ к сетям жертв, кибер-субъекты SVR перемещались по сетям, чтобы получить доступ к учетным записям электронной почты. Целевые учетные записи в нескольких организациях-жертвах включали учетные записи, связанные с ИТ-персоналом. ФБР подозревает, что злоумышленники наблюдали за ИТ-персоналом, чтобы собрать полезную информацию о сетях жертв, определить, обнаружили ли жертвы вторжения, и уклониться от действий по выселению.

Согласно CISA, обнаружение SVR состояло из довольно рутинных задач: аудит файлов журнала «для выявления попыток доступа к привилегированным

сертификатам», мониторинг сетей для закодированных команд PowerShell, профилирование поведения учетных записей для обнаружения необычной активности, указывающей на компрометацию, и использование информации об угрозах для следите за «злоупотреблением учетными данными в облачных средах».

Как предупредил CISA, один из бонусов, о которых вы могли бы разобраться с российским шпионом, - это использование нелепого адреса электронной почты. Хотя мы совершенно уверены, что не русский шпион назвал нас оскорбительными именами с петушиного [.] Li адреса электронной почты в 2016 году, CISA считает: «Хотя кибер-акторы SVR не используют его исключительно, некоторые кибер-персонажи SVR используют службы электронной почты, размещенные на cock [.] li или связанных доменах».

Мы спросили по электронной почте у сопровождающего Петуха Винсента Кэнфилда его мысли о том, что правительство США назвало его укрытием враждебных иностранных шпионов, и воспроизведем любые печатные версии, если он ответит. ®

Namenote

* Поскольку это западный мир информационной безопасности, APT29 имеет около 50 различных названий в зависимости от того, какая компания о них говорит, какой сейчас день недели, солнечно или облачно. Вариации включают The Dukes, Cosy Bear, труднопроизносимый иттрий и т. Д.

Нам говорят, что это маркетинговая стратегия, точно так же, как стартапы, о которых никто не слышал, любят называть себя «ведущим бизнесом в вертикали цифровой обработки редактируемых символов на белом фоне». ***(Gareth Corfield. Here's what Russia's SVR spy agency does when it breaks into your network, says US CISA infosec agency // The Register (https://www.theregister.com/2021/04/27/apt29_russia_svr_tactics_cisa/). 27.04.2021).***

***

Діяльність хакерів та хакерські угруповування

«Кибермошенники начали нанимать «белых хакеров» под видом компаний по кибербезопасности Check Point Software Technologies и Forcepoint. Первой такую практику ввела группировка FIN7, разработав программу, замаскированную под инструмент для пентеста — анализа защищенности сетей. «Белые хакеры» при этом не знают, что работают на преступников. По словам экспертов, атаки такого типа с конца 2020 года идут на американские компании, но вскоре могут переключиться на другие страны, включая Россию.

Известная русскоязычная хакерская группировка FIN7 начала атаковать крупные американские компании, прикидываясь легальной организацией по кибербезопасности, рассказали “Ъ” в Bi.Zone. Для этого злоумышленники разработали программу, которая маскируется под инструмент для анализа защищенности сетей Windows.

Чтобы увеличить охват, FIN7 с прошлого года активно нанимает российских пентестеров («белые хакеры», специалисты по анализу защищенности информационных систем), выдавая себя за представительства израильского разработчика решений по безопасности Check Point Software Technologies и американского разработчика софта Forcepoint.

По словам директора блока экспертных сервисов Bi.Zone Евгения Волошина, нанятые сотрудники даже не подозревают, что работают на злоумышленников. FIN7, уточняет он, интересуют русские специалисты, поскольку они «самые сильные». Пентестерам, подчеркивает господин Волошин, нужно «сохранять бдительность при трудоустройстве».

Пентест — это сознательный взлом системы, чтобы найти ее слабые места. По прогнозу Positive Technologies, по итогам 2020 года объем рынка услуг непрерывного анализа защищенности бизнеса должен был составить 1,5 млрд руб.

В Positive Technologies “Ъ” подтвердили, что кроме кейса FIN7 до 2021 года не наблюдали случаев, когда преступники втягивали в подобные схемы пентестеров. По словам руководителя группы исследований угроз экспертного центра безопасности Positive Technologies (PT Expert Security Center) Дениса Кувшинова, их атаковали иначе и с другими целями. Например, в первом квартале 2021 года участники северокорейской группировки Lazarus писали специалистам по безопасности в соцсетях и мессенджерах, представляясь коллегами, а затем предлагали прочитать статью в личном блоге.

Если жертва пользовалась браузером Google Chrome, поясняет господин Кувшинов, при переходе в блог эксплуатировалась уязвимость нулевого дня, и компьютер жертвы оказывался зараженным. Суть была в том, что на устройствах специалистов по безопасности могла находиться важная для хакеров конфиденциальная информация.

Теперь же «белые хакеры» сами становятся частью атаки, ликвидируя кадровый дефицит у кибермошенников.

Глава представительства Check Point в России и СНГ Василий Дягилев подтверждает, что проблема становится актуальной. В данном случае, по его мнению, злоумышленники рассчитывают воспользоваться доверчивостью компаний, которые стремятся сэкономить на проведении нормального пентеста, «название известного бренда позволяет им войти в доверие». Во время теста на проникновение или в результате удачного обнаружения брешей в защите специалисты часто получают высокий уровень привилегий для доступа к системе.

Группировка FIN7 основана в 2013 году и известна атаками с целью финансовой выгоды либо шпионажа. Мишенью преступников в России и на постсоветском пространстве были в основном банки и платежные системы, рассказывает ведущий специалист по компьютерной криминалистике Group-IB Олег Скулкин. В 2019 году расследование в отношении группировки проводила «Лаборатория Касперского»: исследователи обнаружили связь хакеров с другой известной группой Carbanak. В 2020 году FIN7 принимала активное участие в Big Game Hunting — атаках на крупные компании с целью вымогательства выкупа за расшифровку данных, говорит Олег Скулкин.

FIN7 переключились на атаки с использованием программ-вымогателей, так как они проще в реализации и могут принести хакерам такую же прибыль, полагает господин Скулкин…». ***(Юлия Степанова. Повзломались и согласились. Специалисты по кибербезопасности поработали на хакеров // Газета "Коммерсантъ" (https://www.kommersant.ru/doc/4782204). 21.04.2021).***

***

«Группа хакеров, получившая название REvil, нашла лазейку в компьютерной сети тайваньского сборщика Quanta, одной из азиатских компаний, с которой Apple работает для производства своих компьютеров.

По крайней мере, так объявляет эта российская сеть, которая, согласно ее заявлениям, украла бы документы американского бренда, включая планы сборки MacBook и iMac. 20 апреля на хакерском сайте было размещено несколько достоверных диаграмм.

По данным американских СМИ Пластинка, Revil угрожая опубликовать другую конфиденциальную информацию, если компания Apple не платит выкуп в размере $ 50 млн (около 41,5 млн евро) на 1 - м мая. Эта группа хакеров предпринимает не первую попытку, поскольку в последние недели она объявила, что стоит за организованной атакой на производителей компьютеров Acer, а также за атакой на компьютеры Фармацевтическая группа Пьера Фабра.

В заявлении информационному агентству Bloomberg, Кванта подтвердила, что подверглась компьютерной атаке. По словам сборщика, пираты проникли бы только на «небольшое количество серверов» и не парализовали бы его производственные линии. Компания заявила, что работает над повышением безопасности своих сетей.

Конфиденциальные документы

В документах, опубликованных REvil, по нашим наблюдениям, значатся планы MacBook, доступные на рынке с 2020 года. Эти планы, однако, сопровождаются чрезвычайно точными и подробными инструкциями по сборке.

Но REvil также раскрывает планы относительно нового поколения настольных компьютеров iMac, о которых было объявлено в тот же день, за три недели до их выпуска в магазинах, намеченного на середину мая. По-прежнему среди этих документов есть планы на будущий MacBook, который, согласно американскому информационному изданию The Verge, будет отличаться дизайном от нынешней модели.

Что касается документов, которые не разглашаются, Quanta и Apple - единственные, кто точно знает, что в них содержится. Если планы по выпуску особо радикальных новых моделей будут выпущены, ущерб может оказаться значительным для Apple». ***(Nicolas Six. L'assembleur Quanta, sous-traitant d'Apple, frappé par une cyberattaque // SUIVEZ LE MONDE (https://www.lemonde.fr/economie/article/2021/04/22/apple-frappe-par-une-attaque-au-rancongiciel_6077679_3234.html). 22.04.2021).***

***

«Популярный хакерский форум OGUsers был взломан в четвертый раз за два года, и теперь хакеры продают базу данных сайта, содержащую пользовательские записи и личные сообщения.

OGUsers - это хакерский форум, известный продажей украденных учетных записей социальных сетей, взломанных с помощью атак с заменой SIM-карт, атак с заполнением учетных данных и другими способами.

Совсем недавно Министерство юстиции США обвинило членов OGUsers в их роли в череда успешных взломов проверенных учетных записей Twitter, используемых для продвижения мошенничества с криптовалютой.

OGUsers, взломанные ранее в этом месяце

На прошлой неделе компания KELA, занимающаяся киберинтразведкой, написала в Твиттере, что администратор форума OGUsers подтвердил, что сайт был взломан после того, как хакеры загрузили веб-оболочку на свой сервер.

В то время администратор OGUsers не был уверен, что база данных была взломана, но вскоре после этого участники конкурирующего хакерского форума начали продавать украденную базу данных OGUsers за 3000 долларов.

Источник, знакомый с атакой, сообщил BleepingComputer, что OGusers был взломан 11 апреля 2021 года и что злоумышленники получили доступ к полному дампу базы данных форума. Этот дамп включает записи пользователей и личные сообщения примерно 350 000 участников OGUsers.

Этот источник сообщил BleepingComputer, что OGUsers использует множество подключаемых модулей, содержащих уязвимости, которые злоумышленники могут объединить в цепочку для «оболочки сайта».

Виталий Кремез, генеральный директор компании Advanced Intel, занимающейся кибербезопасностью, сказал нам, что утечки баз данных на криминальных форумах могут принести пользу правоохранительным органам и исследователям в области безопасности.

«Эта предполагаемая утечка OGUsers может потенциально выявлять киберпреступников через их регистрационные учетные записи электронной почты и IP-адреса и ссылаться на их настоящие личности».

«Предыдущие утечки OGUsers выявили важные улики, которые помогли раскрыть киберпреступные операции, особенно те, которые связаны с мошенничеством с захватом криптовалютных учетных записей и операциями по замене SIM-карт», - сказал Кремез BleepingComputer.

Множественные взломы в прошлом

Это не первый случай, когда OGUsers взламывают, а их базы данных продают другие хакеры.

В мае 2019 года администратор OGUsers сообщил своим пользователям, что они были взломаны после того, как хакеры использовали пользовательский плагин. Брайан Кребс сообщил, что OGUsers снова взломали в ноябре 2020 года.

Наконец, они также были взломаны в апреле 2020 года после того, как злоумышленник загрузил веб-оболочку через функцию форума загрузки аватаров.

«Мы полагаем, что мы, вероятно, увидим, что многие участники OGUsers перейдут в другие сообщества - и, возможно, даже создадут новые - учитывая как слабую операционную безопасность, так и ущерб, нанесенный бренду OG

мошенниками и другими преступными игроками», - Дэвиди Кармиэль, технический директор KELA, совместно с BleepingComputer.

Когда мы спросили нашего источника в хакерском сообществе, считают ли они, что OGUsers снова будут взломаны, они немедленно ответили «Да». ***(Lawrence Abrams. Fourth time's a charm - OGUsers hacking forum hacked again // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fourth-times-a-charm-ogusers-hacking-forum-hacked-again/). 28.04.2021).***

***

Вірусне та інше шкідливе програмне забезпечення

«Агентство по кибербезопасности и безопасности инфраструктуры США (CISA) на этой неделе опубликовало подробную информацию о дополнительных вредоносных программах, обнаруженных на скомпрометированных серверах Microsoft Exchange, а именно о веб-оболочках China Chopper и программе-вымогателе DearCry.

Операторы вредоносного ПО нацелены на серверы Exchange через серию уязвимостей, о которых стало известно 3 марта, в тот же день, когда Microsoft выпустила для них исправления. Ошибки были устранены до публичного объявления, и вскоре после этого возросла активность, связанная с ними.

3 марта CISA опубликовала уведомление об использовании уязвимостей Exchange, а на этой неделе анонсировала обновление для этого предупреждения, добавив отчеты об анализе вредоносного ПО (MAR), которые включают информацию о дополнительных атаках.

Первая из них содержит подробную информацию о веб-оболочках China Chopper, которые были обнаружены на серверах Exchange после первоначального взлома через вышеупомянутые уязвимости и которые предоставляют злоумышленникам контроль над зараженной машиной.

В CISA отмечает, что в общей сложности было идентифицировано 10 веб-оболочек, но их не следует рассматривать как исчерпывающий список веб-оболочек, которые злоумышленники используют в атаках, направленных на серверы Exchange.

Кроме того, CISA предупреждает о нападениях на Microsoft Exchange, которые пытаются сбросить программу-вымогатель DearCry на уязвимые серверы.

DearCry, также известное как DoejoCrypt, является первым семейством программ-вымогателей, которые нацелены на серверы Exchange. Уже более двух недель программа-вымогатель Black Kingdom / Pydomer предпринимает аналогичные попытки.

В новые общие MAR, CISA включила тактики, техники и процедуры (TTP) и индикаторы компрометации (IOC), чтобы помочь защитникам выявлять и устранять потенциальные угрозы.

Однако атаки на серверы Microsoft Exchange гораздо более разнообразны и в некоторых случаях также включают использование криптомайнеров. Фактически,

сама Microsoft предупредила примерно две недели назад об активности, связанной с ботнетом с криптовалютой Lemon Duck.

Теперь Sophos сообщает, что использование серверов Exchange для майнинга криптовалют началось еще 9 марта, через несколько часов после выпуска обновлений Microsoft Patch Tuesday, направленных на устранение эксплуатируемых уязвимостей. С тех пор, как сообщает охранная компания, неизвестный злоумышленник взламывает серверы, чтобы развернуть вредоносный майнер Monero.

Однако эта атака выделяется тем, что сама вредоносная полезная нагрузка размещается на скомпрометированном сервере Exchange и извлекается с помощью команды PowerShell. Полезная нагрузка маскируется под законную утилиту с именем QuickCPU.

В течение нескольких дней майнер был загружен на несколько взломанных серверов, что привело к значительному скачку вывода криптовалюты. Активность продолжается, хотя и гораздо более медленными темпами, поскольку майнер потерял часть зараженных серверов». ***(Ionut Arghire. CISA Details Malware Found on Hacked Exchange Servers // Wired Business Media (https://www.securityweek.com/cisa-details-malware-found-hacked-exchange-servers). 13.04.2021).***

***

«6 апреля 2021 года DocuSign выпустила оповещение, уведомляющее пользователей о новом вредоносном хакерском инструменте, имитирующем DocuSign, для внедрения вредоносных программ в системы жертв. Согласно Alert, инструмент создания документов, получивший название EtterSilent, «создает документы Microsoft Office, содержащие вредоносные макросы, или пытается использовать известную уязвимость Microsoft Office (CVE-2017-8570) для загрузки вредоносного ПО на компьютер жертвы. Эта деятельность исходит от злонамеренных сторонних источников и не исходит от платформы DocuSign».

В предупреждении далее говорится: «На сегодняшний день было замечено, что вредоносные документы доставляют множество различных семейств вредоносных программ, таких как Trickbot, QBot, Bazar, IcedID и Ursnif. Такие типы вредоносных программ обычно доставляются жертвам с помощью фишинговых атак».

DocuSign предоставляет индикаторы взлома в предупреждении, доступ к которым можно получить здесь.

Поскольку EtterSilent выпускается с использованием макросов, стоит предупредить пользователей компании о том, что загрузка макросов очень подозрительна и что они могут пожелать обратиться к специалистам по информационным технологиям, прежде чем загружать макросы, включенные в документ или ссылку. Если компания регулярно использует DocuSign, предупреждение пользователей об этой схеме может помочь им не стать жертвой». ***(Linn Foster Freedman. DocuSign Alert: New Malicious Hacking Tool Mimicking DocuSign Observed // Robinson & Cole LLP***

(https://www.dataprivacyandsecurityinsider.com/2021/04/docusign-alert-new-malicious-hacking-tool-mimicking-docusign-observed/). 08.04.2021).

***

«Исследователи разоблачили банковского трояна, поражающего корпоративные цели по всей Бразилии.

Во вторник ESET опубликовала рекомендацию по вредоносному ПО, разработка которого началась с 2018 года.

Троянец, получивший название Janeleiro, похоже, ориентирован на Бразилию как на охотничьи угодья и использовался в кибератаках против корпоративных игроков в таких секторах, как здравоохранение, машиностроение, розничная торговля, финансы и производство. Операторы также пытались использовать вредоносное ПО при проникновении в правительственные системы.

По словам исследователей, троянец похож на другие, которые в настоящее время действуют по всей стране, такие как Casbaneiro, Grandoreiro и Mekotio, но это первый обнаруженный троянец, написанный на.NET, а не на Delphi, который обычно предпочитают.

Фишинговые электронные письма, рассылаемые небольшими партиями, рассылаются корпоративным целям, якобы связанными с неоплаченными счетами. Эти сообщения содержат ссылки на взломанные серверы и на загрузку архива.zip, размещенного в облаке. Если жертва распакует этот архивный файл, установщик MSI для Windows загружает основную DLL троянца.

«В некоторых случаях эти URL-адреса распространялись как Janeleiro, так и другими банкирами Delphi в разное время», - сообщает ESET. «Это говорит о том, что либо у различных преступных группировок используется один и тот же провайдер для рассылки спама и для размещения своих вредоносных программ, либо это одна и та же группа. Мы еще не определили, какая гипотеза верна».

Троянец сначала проверит геолокацию IP-адреса целевой системы. Если код страны отличается от Бразилии, вредоносная программа завершит работу. Однако, если проверка пройдена, вредоносная программа соберет различные данные операционной системы и захватит адрес своего командно-управляющего (C2) сервера со специальной страницы GitHub.

Janeleiro используется для создания фальшивых всплывающих окон «по запросу», например, когда ключевые слова, связанные с банковскими операциями, обнаруживаются на взломанной машине. Эти всплывающие окна созданы так, чтобы они создавались некоторыми из крупнейших банков Бразилии, и они запрашивают конфиденциальные и банковские данные от жертв.

Список команд вредоносной программы включает в себя параметры для управления окнами, уничтожения существующих сеансов браузера, таких как запущенные в Google Chrome, захвата экранов, кейлоггеров и захвата данных буфера обмена, среди других функций.

Оператор троянца, похоже, предпочитает практический подход и может управлять окнами удаленно в режиме реального времени.

Большинство операторов вредоносных программ, по крайней мере, делают токен-попытку скрыть свою деятельность. В этом случае обфускация кода проста,

но не предпринимается попыток обойти существующее программное обеспечение безопасности и настраиваемое шифрование.

Оператор использует GitHub, репозиторий кода, для размещения файлов, содержащих списки серверов C2, для управления заражением троянскими программами. Эти репозитории обновляются ежедневно.

По состоянию на март четыре варианта Janeleiro были обнаружены в дикой природе, хотя два имеют один и тот же внутренний номер версии. Некоторые образцы были упакованы вместе со средством для кражи паролей при атаках, что предполагает, что «группа, стоящая за Janeleiro, имеет в своем арсенале другие инструменты», согласно команде.

ESET сообщает, что GitHub был проинформирован об учетной записи злоумышленника и злоупотреблении платформой. Страница теперь отключена, а владелец заблокирован.

«GitHub ценит вклад нашего сообщества исследователей в области безопасности и стремится исследовать обнаруженные проблемы безопасности», - сказал ZDNet представитель GitHub. «Мы отключили страницу в соответствии с нашими Политиками допустимого использования, после того, как поступило сообщение о том, что она использовала нашу платформу злонамеренно». ***(Charlie Osborne. Meet Janeleiro: a new banking Trojan striking company, government targets // ZDNet (https://www.zdnet.com/article/meet-janeleiro-a-new-banking-trojan-striking-corporate-targets/). 06.04.2021).***

***

«Исследователи обнаружили, что несколько вариантов семейства вредоносных программ ботнета на основе Gafgyt Linux включают код печально известного ботнета Mirai.

Gafgyt (он же Bashlite) - ботнет, впервые обнаруженный в 2014 году. Он нацелен на уязвимые устройства Интернета вещей (IoT), такие как маршрутизаторы Huawei, маршрутизаторы Realtek и устройства ASUS, которые затем использует для запуска крупномасштабных распределенных атак типа «отказ в обслуживании» (DDoS). Он также часто использует известные уязвимости, такие как CVE-2017-17215 и CVE-2018-10561, для загрузки полезных данных следующего этапа на зараженные устройства.

Согласно исследованию Uptycs, опубликованному в четверг, последние варианты теперь включают несколько модулей на основе Mirai, а также новые эксплойты. Варианты Mirai и его повторное использование кода стали более объемными, поскольку исходный код ботнета IoT был выпущен в октябре 2016 года.

Согласно исследованию, возможности, заимствованные у Mirai, включают в себя различные методы для проведения DDoS-атак:

HTTP-флуд, при котором ботнет отправляет большое количество HTTP-запросов на целевой сервер, чтобы завалить его;

UDP-флуд, при котором ботнет отправляет несколько пакетов UDP на сервер жертвы в качестве средства его исчерпания;

Различные атаки TCP-флуда, которые используют обычное трехстороннее TCP-рукопожатие, сервер-жертва получает большое количество запросов, в результате чего сервер перестает отвечать;

И модуль STD, который отправляет случайную строку (из жестко запрограммированного массива строк) на определенный IP-адрес.

Между тем, как выяснил Uptycs, последние версии Gafgyt содержат новые подходы к достижению начальной компрометации IoT-устройств; это первый шаг к превращению зараженных устройств в ботов для последующего выполнения DDoS-атак на целевые IP-адреса. К ним относятся скопированный Mirai модуль для перебора Telnet и дополнительные эксплойты для существующих уязвимостей в устройствах Huawei, Realtek и GPON.

Согласно анализу, эксплойт Huawei (CVE-2017-17215) и эксплойт Realtek (CVE-2014-8361) используются для удаленного выполнения кода (RCE), чтобы получить и загрузить полезную нагрузку Gafgyt.

«Бинарный файл вредоносного ПО Gafgyt включает эксплойты RCE для маршрутизаторов Huawei и Realtek, с помощью которых двоичный файл вредоносного ПО с помощью команды wget извлекает полезную нагрузку», - сообщает Uptycs. «[Он] дает разрешение на выполнение полезной нагрузки с помощью команды chmod, [и] выполняет полезную нагрузку».

Эксплойт GPON (CVE-2018-10561) используется для обхода аутентификации в уязвимых маршрутизаторах Dasan GPON; здесь двоичный файл вредоносной программы следует тому же процессу, но также может удалить полезную нагрузку по команде.

«IP-адреса, используемые для получения полезных данных, как правило, были открытыми каталогами, в которых злоумышленники размещали вредоносные полезные данные для различных архитектур», - добавили исследователи.

Множество вариантов ботнета IoT

Ботнеты Интернета вещей, такие как Gafgyt, постоянно развиваются. Например, в марте исследователи обнаружили, что, по их словам, это первый вариант семейства ботнетов Gafgyt, скрывающий свою деятельность с помощью сети Tor.

Не исчез и Mirai: недавно был обнаружен новый вариант ботнета, нацеленный на множество уязвимостей в непропатченных устройствах D-Link, Netgear и SonicWall. С середины февраля этот вариант был нацелен на шесть известных уязвимостей и три ранее неизвестных, чтобы заразить системы и добавить их в ботнет.

Это только последний вариант Mirai, который обнаружился. В прошлом году версия, получившая название Mukashi, была замечена с использованием уязвимости, связанной с внедрением команд до аутентификации, обнаруженной в устройствах хранения Zyxel NAS.

«Авторы вредоносных программ не всегда могут вводить новшества, и исследователи часто обнаруживают, что авторы вредоносных программ копируют и повторно используют утекший исходный код вредоносных программ», - говорят исследователи Uptycs.

Исследователи рекомендуют, чтобы защититься от заражения ботнетами такого типа, пользователи должны регулярно отслеживать подозрительные процессы, события и сетевой трафик, порождаемые выполнением любого ненадежного двоичного файла. Кроме того, пользователи должны обновлять все системы и прошивки до последних выпусков и исправлений». ***(Tara Seals. Gafgyt Botnet Lifts DDoS Tricks from Mirai // Threatpost (https://threatpost.com/gafgyt-botnet-ddos-mirai/165424/). 15.04.2021).***

***

«По словам исследователей, вредоносная программа BazarLoader усиливает доверие сотрудников к инструментам для совместной работы, таким как Slack и BaseCamp, в сообщениях электронной почты со ссылками на полезные нагрузки вредоносных программ.

А во вторичной кампании, нацеленной на потребителей, злоумышленники добавили в цепочку атаки элемент голосового вызова.

BazarLoader загрузчик, написанный на C ++, имеет основную функцию загрузки и выполнения дополнительных модулей. BazarLoader впервые был замечен в дикой природе в апреле прошлого года - и с тех пор исследователи наблюдали как минимум шесть вариантов, «сигнализирующих об активном и продолжающемся развитии».

Недавно было замечено, что его использовали в качестве промежуточного вредоносного ПО для программ-вымогателей, в частности Ryuk.

«С упором на цели в крупных предприятиях, BazarLoader потенциально может быть использован для проведения последующей атаки вымогателей», - говорится в сообщении Sophos, опубликованном в четверг

Кибератаки злоупотребляют Slack и BaseCamp

По словам исследователей Sophos, в ходе первой обнаруженной кампании злоумышленники нацелены на сотрудников крупных организаций с помощью электронных писем, в которых содержится важная информация, касающаяся контрактов, обслуживания клиентов, счетов-фактур или начисления заработной платы.

«Один образец спама даже попытался замаскироваться под уведомление об увольнении сотрудника с работы», - сообщает Sophos.

Ссылки в электронных письмах размещаются в облачном хранилище Slack или BaseCamp, а это означает, что они могут выглядеть законными, если цель работает в организации, которая использует одну из этих платформ. В эпоху удаленной работы есть хорошие шансы, что это так.

«Злоумышленники поместили URL-адрес, указывающий на один из этих хорошо известных легитимных веб-сайтов, в основной части документа, придавая ему вид убедительности», - говорят исследователи. «Затем URL-адрес может быть дополнительно запутан с помощью службы сокращения URL-адресов, чтобы сделать менее очевидным, что ссылка указывает на файл с расширением.EXE».

Если цель нажимает на ссылку, BazarLoader загружается и запускается на машине жертвы. Ссылки обычно указывают непосредственно на исполняемый файл с цифровой подписью с изображением Adobe PDF в качестве значка. Как

отмечают исследователи, файлы обычно увековечивают уловку с такими именами, как presentation-document.exe, preview-document- [номер].exe или Annualreport.exe.

Эти исполняемые файлы при запуске внедряют полезную нагрузку DLL в законный процесс, такой как командная оболочка Windows, cmd.exe.

«Вредоносное ПО, работающее только в памяти, не может быть обнаружено при сканировании файловой системы средством защиты конечных точек, поскольку оно никогда не записывается в файловую систему», - пояснили исследователи. «Сами файлы даже не используют законный суффикс файла.DLL, потому что Windows, похоже, не заботится о том, чтобы он у них был; ОС запускает файлы в любом случае».

Кампания BazarCall

Во второй кампании Sophos обнаружил, что в спам-сообщениях нет ничего подозрительного: в теле письма нет никакой личной информации, нет ссылок и файловых вложений.

«Все сообщения утверждают, что бесплатная пробная версия онлайн-службы, которую получатель якобы использует в настоящее время, истекает через день или два и включает номер телефона, по которому получатель должен позвонить, чтобы отказаться от дорогостоящей платной услуги. обновление», - пояснили исследователи.

Если цель решает взять трубку, дружелюбный человек на другой стороне дает ему адрес веб-сайта, где потенциальная жертва может предположительно отказаться от подписки на услугу.

«Хорошо продуманные и профессионально выглядящие веб-сайты скрывают кнопку отказа от подписки на странице часто задаваемых вопросов», - говорит Sophos. «При нажатии этой кнопки появляется вредоносный документ Office (документ Word или электронная таблица Excel), который при открытии заражает компьютер той же вредоносной программой BazarLoader».

Первоначально сообщения утверждали, что они исходят от компании под названием Medical Reminder Service, и включают в себя номер телефона в теле сообщения, а также адрес реального офисного здания, расположенного в Лос-Анджелесе. Но в середине апреля в сообщениях использовалась приманка, связанная с поддельной платной онлайн-библиотекой под названием BookPoint.

Строки темы, вращающиеся вокруг BookPoint, также ссылаются на длинный номер или код, который пользователей просят ввести, чтобы «отказаться от подписки».

Что касается процедуры заражения, злоумышленники в этих так называемых кампаниях «BazarCall» доставляют вооруженные документы Microsoft Office, которые вызывают команды для удаления и выполнения одной или нескольких полезных библиотек DLL.

Подключение к Trickbot?

Исследователи подозревали, что BazarLoader может быть связан или создан операторами TrickBot. TrickBot - еще одна вредоносная программа-загрузчик первого уровня, которая часто используется в кампаниях вымогателей.

Sophos проверил соединение и обнаружил, что две вредоносные программы используют одну и ту же инфраструктуру для управления и контроля.

«Из того, что мы могли сказать, двоичные файлы вредоносного ПО [BazarLoader], работающие в лабораторной сети, не имеют ничего общего с TrickBot», - говорится в сообщении. «Но они действительно обменивались данными с IP-адресом, который исторически использовался совместно обоими семействами вредоносных программ. Конечно, многие люди изучали эту связь в прошлом».

В любом случае, BazarLoader, похоже, находится на ранней стадии разработки и не так сложен, как более зрелые семейства, такие как TrickBot, добавили исследователи.

Например, «хотя ранние версии вредоносного ПО не были обфусцированы, более свежие образцы, по-видимому, зашифровывают строки, которые могут раскрыть предполагаемое использование вредоносного ПО», - заявили они». ***(Tara Seals. BazarLoader Malware Abuses Slack, BaseCamp Clouds // Threatpost (https://threatpost.com/bazarloader-malware-slack-basecamp/165455/). 16.04.2021).***

***

«Поддерживаемая Северной Кореей хакерская группа Lazarus использовала новое вредоносное ПО с возможностями бэкдора, получившее название Vyveva, в целевых атаках на южноафриканскую логистическую компанию.

Как выяснили исследователи ESET, Vyveva впервые использовалась в атаке в июне 2020 года, но дальнейшие доказательства показывают, что Lazarus развертывал ее в предыдущих атаках, начиная как минимум с декабря 2018 года.

Хотя ESET обнаружил только две машины, зараженные этой вредоносной программой, обе принадлежали одной и той же южноафриканской транспортной компании, бэкдор, вероятно, использовался в других целевых шпионских кампаниях с тех пор, как он был впервые развернут в дикой природе.

«У Vyveva есть несколько общих черт в коде со старыми образцами Lazarus, которые обнаруживаются с помощью технологии ESET», - сказал в опубликованном сегодня отчете исследователь безопасности Филип Юрчацко.

«Однако на этом сходство не заканчивается: использование поддельного протокола TLS в сетевых коммуникациях, цепочки выполнения из командной строки и методы использования шифрования и служб Tor указывают на Lazarus. Следовательно, мы можем отнести Vyveva к этому APT группа с высокой степенью уверенности».

Бэкдор сделан в Северной Корее

Вредоносная программа обладает обширным набором возможностей кибершпионажа, позволяющих операторам Lazarus собирать и экспортировать файлы с зараженных систем на серверы под их контролем, используя анонимную сеть Tor в качестве безопасного канала связи.

Lazarus также может использовать Vyveva для доставки и выполнения произвольного вредоносного кода в любой скомпрометированной системе в сети жертвы.

Среди других «особенностей» бэкдора есть поддержка команд временной метки, что позволяет его операторам манипулировать датой любого файла,

используя метаданные из других файлов в системе или устанавливая случайную дату между 2000 и 2004 годами, чтобы скрыть новые или измененные файлы.

Хотя бэкдор будет подключаться к своему серверу управления и контроля (C2) каждые три минуты, он также использует сторожевые таймеры, предназначенные для отслеживания вновь подключенных дисков или активных пользовательских сеансов, чтобы инициировать новые подключения C2 при новом сеансе или событиях диска.

«Vyveva представляет собой еще одно дополнение к обширному арсеналу вредоносных программ Lazarus», - добавил Юрчацко. «Атака на компанию в Южной Африке также демонстрирует широкий географический охват этой APT-группы»…». ***(Sergiu Gatlan. North Korean hackers use new Vyveva malware to attack freighters // Bleeping Computer (https://www.bleepingcomputer.com/news/security/north-korean-hackers-use-new-vyveva-malware-to-attack-freighters/). 08.04.2021).***

***

«Согласно данным, полученным и рассчитанным Finbold, в 2021 году во всем мире ежедневно будет регистрироваться около 604059 новых вредоносных программ (вредоносных программ) и потенциально нежелательных приложений (PUA).

Эти оценки основаны на уже зарегистрировано 61,01 млн новых вредоносных программ в период с января 1 - го, 2021 и 11 апреля - го, 2021 В январе этот показатель был на уровне 17,63 млн, в то время как в феврале, 17,85 миллионов новых вредоносных программ было зафиксировано. В марте их было 19,2 миллиона, а на 11 апреля 2021 года было зарегистрировано 6,33 миллиона новых вредоносных программ.

Исходя из темпов роста, к концу 2021 года будет зарегистрировано около 220 миллионов новых вредоносных программ. Цифра представляет собой рост на 56,86% с 137,7 миллиона, зарегистрированных в прошлом году.

Степень серьезности вредоносных программ, зарегистрированных в этом году, демонстрируется по сравнению с прошлогодними случаями. Всего за три с половиной месяца вредоносное ПО в этом году составляет 44,3% от 137,7 млн новых вредоносных программ на 2020 год.

Объем вредоносного ПО резко возрастает на фоне пандемии

В отчете освещаются обстоятельства, которые сделали возможным появление большого количества вредоносных программ и PUA. Согласно отчету исследования, «пандемия вызвала массовые сбои в бизнес-операциях, и многие организации сосредоточились на том, как оставаться на плаву в условиях экономического кризиса. В этом случае отвлекается большинство организаций и частных лиц. Поэтому высока вероятность снятия охраны. Такая среда открывает двери для исследователей вредоносных программ».

На протяжении многих лет предпринимались попытки защитить устройства от вредоносных программ. Однако в отчете отмечается, что киберпреступники также развиваются: «Хотя данные свидетельствуют о большом количестве зарегистрированных новых вредоносных программ, важно отметить, что

киберпреступники также используют изощренность при распространении вредоносных программ.

По мере того как организации и отдельные лица внедряют механизмы для предотвращения вредоносных программ, киберпреступники изучают передовые тактики уклонения, которые значительно затрудняют обнаружение».

Большое количество зарегистрированных новых вредоносных программ представляет собой серьезную проблему для обнаружения угроз и реагирования на готовность организации к киберугрозам. Для борьбы с вредоносными программами необходимы координация и повышение осведомленности». ***(Anasia D'mello. Over 600,000 new malicious programs registered globally every day in 2021 // IoT Now - Internet of Things News (https://www.iot-now.com/2021/04/12/109131-over-600000-new-malicious-programs-registered-globally-every-day-in-2021/). 12.04.2021).***

***

«На выходных Sonatype обнаружила довольно уникальный образец вредоносного ПО, опубликованный в реестре npm, в течение дня после его выпуска на npm.

Вредоносная программа существует в npm-пакете brandjacking под названием «web-browserify» и имитирует законный компонент «browserify».

Нам доверяют сотни тысяч разработчиков NodeJS, Browserify получает более 1,3 миллиона загрузок еженедельно только на npm.

Популярность Browserify связана с тем, что это инструмент JavaScript с открытым исходным кодом, который позволяет разработчикам писать кроссплатформенные модули в стиле NodeJS, которые компилируются для использования в браузере.

Но вредоносный пакет «web-browserify», с другой стороны, злоупотребляет законными компонентами npm, чтобы связать в себе вредоносный, трудно обнаруживаемый исполняемый файл Linux и Mac.

Следует отметить, что пакет, по-видимому, специально разработан для отдельных разработчиков NodeJS, судя по тому, как он действует после загрузки, и выбору операционных систем, на которые он нацелен.

Вредоносное ПО запускается сразу после установки разработчиками веб-браузера.

Автоматическая система обнаружения вредоносных программ от Sonatype, Release Integrity, часть нашего Nexus Intelligence следующего поколения, отметила компонент npm «web-browserify» как подозрительный в минувшие выходные.

При более внимательном рассмотрении команда Sonatype Security Research подтвердила, что пакет является вредоносным, и сразу же добавила его к нашим данным.

Компонент npm «web-browserify», который сейчас отключен, существовал на npm в виде архива.TGZ (типично для компонентов npm) только с одной версией (1.0.0) размером около 27 МБ.

Файл «postinstall.js» просто извлекает загадочный архив «run.tar.xz» (показанный выше), вложенный в архив TGZ компонента «web-browserify».

Кроме того, «run.tar.xz» содержит 64-битный исполняемый файл ELF под названием «run», который может работать как в операционных системах Linux, так и в Mac.

Формат исполняемых и связываемых файлов (ELF) - это общий формат для исполняемых двоичных файлов и библиотек на основе Unix.

Как видно из строки 6 «package.json» выше, сценарий postinstall запускает этот двоичный файл «run» и очищает (временный) извлеченный каталог с «run», содержащимся в нем.

Но это не останавливает вредоносное ПО, и здесь начинается самое интересное.

Извлеченный исполняемый двоичный файл огромен, имеет размер около 120 МБ и включает в себя сотни законных компонентов npm.

Фактически, вредоносная программа почти полностью создается из компонентов с открытым исходным кодом и использует эти легитимные компоненты npm для проведения обширных разведывательных операций.

Следует отметить, что исполняемый двоичный файл выполняет свои гнусные действия таким образом, который может показаться вполне приемлемым для антивирусных продуктов. Таким образом, на момент написания он имел идеальный нулевой показатель обнаружения VirusTotal.

Как только вредоносная программа запускается, она выдает несколько команд «systemctl» для остановки критически важных системных служб и дополнительно удаляет каталог / etc / systemd / system /, содержащий символические ссылки на демонов и системных служб, включая антивирус.

Далее вредоносная программа пытается очистить сам каталог / etc /, который содержит самый обширный набор важных файлов конфигурации системы, хэши паролей, правила DNS и т. Д., И был назван «нервным центром вашей системы».

Затем вредоносная программа копирует себя в / etc / rot1, где получает постоянство и запускается при каждой загрузке.

Однако для облегчения вышеупомянутых действий «запуск» потребуются повышенные (root) привилегии, которые он запрашивает у пользователя сразу после запуска.

Для пользователя (вероятно, разработчика) это могло бы показаться, как если бы это был компонент npm «web-browserify», который запрашивал эти разрешения в качестве постустановки. Последовательность запуска триггеров «запустить» сразу после установки компонента.

Мы заметили, что исполняемый файл ELF содержит код в кодировке base64, который мы проследили до еще одного компонента npm «sudo-prompt».

sudo-prompt - это модуль npm, который может быть включен разработчиками в приложения NodeJS для запроса административных разрешений у пользователя.

Не случайно и то, что sudo-prompt является кроссплатформенным.

Выбор «sudo-prompt» кажется преднамеренным для автора, разрабатывающего вредоносное ПО для Mac, Linux и других дистрибутивов на основе Unix, которые наиболее часто используются разработчиками NodeJS.

Обширная дактилоскопия, разведка и кража данных

Как указывалось ранее, многомегабайтный исполняемый файл «run» объединяет в себе сотни легитимных компонентов npm для выполнения своей работы.

Одним из таких компонентов является «системная информация», возвращающая обширную информацию о машине, от простого имени операционной системы, имени пользователя и информации, связанной с процессором / графическим процессором, до более подробной информации о любых изображениях dockerImages, запущенных в системе или подключенных устройствах Bluetooth.

Мы наблюдали, как исполняемый двоичный файл каждые несколько секунд устанавливает HTTP-соединения с доменом me.ejemplo [.] Me, который использует известного поставщика облачного хостинга, для кражи части этой информации.

Опять же, выбор самого домена был разумным, поскольку ejemplo в переводе с испанского означает «например». Это может создать впечатление, что ejemplo [.] Me - это просто тестовый домен, очень похожий на example.com.

Бинарный «запуск» обширен по своей природе, он содержит код, заимствованный из сотен компонентов, обеспечивающих такие возможности, как снятие отпечатков пальцев и разведка для обнаружения виртуализации, т.е. если «запуск» запускается на виртуальной машине (ВМ).

Тактика уклонения, примененная вредоносным ПО, сделала его особенно сложным для анализа, поэтому для выяснения поведения этого двоичного файла использовалась комбинация методов статического и динамического анализа.

По крайней мере, мы можем подтвердить попытки вредоносного ПО повредить критически важные системные файлы, провести обширную разведку и снятие отпечатков пальцев, а также выполнить кражу данных, но обширный характер кода, встроенного в вредоносное ПО, указывает на то, что в нем еще предстоит открыть грядущие дни.

Развитие атак на цепочки поставок с открытым исходным кодом требует повышенной защиты

Еще раз, этот конкретный пакет указывает на то, что разработчики стали новой мишенью для злоумышленников из-за программного обеспечения, которое они пишут.

web-browserify стремится захватить систему разработчика и делает это с помощью счастливой командной строки sudo, разработанной с теми же инструментами, которые используются в законных пакетах, чтобы не попасть под радар ничего не подозревающего разработчика.

Снова и снова, Sonatype было отслеживание не только критических уязвимостей и атак цепи поставок следующего поколения, но новый brandjacking, cryptomining и Typosquatting вредоносное скрываясь в репозиториях.

Более того, мы также определили пакеты-подражатели путаницы зависимостей, которые на самом деле были вредоносными ицелевые приложения, относящиеся к известным технологическим компаниям.

Все это требует не только должной осмотрительности и удачи - это требует опыта опытных профессионалов в области безопасности и сотен терабайт данных. Чтобы не отставать от темпов мутаций вредоносных программ, Sonatype

анализирует каждый недавно выпущенный пакет npm, чтобы обеспечить безопасность разработчиков.

Наша автоматизированная система обнаружения вредоносных программ на базе искусственного интеллекта / машинного обучения, целостность релизов и группа исследователей безопасности мирового класса помогут вам оставаться активными и защищать цепочки поставок программного обеспечения от предстоящих атак. Release Integrity предсказывает вероятный вредоносный компонент на основе анализа прошлых атак на цепочку поставок и более пяти десятков «сигналов», которые позволяют выявить новые потенциальные атаки до того, как их обнаружат исследователи безопасности.

Прежде всего, новейший брандмауэр Nexus помогает оставаться защищенным от атак на основе зависимости / путаницы в пространстве имен, блокируя как подозрительные компоненты, так и зависимости с конфликтующими именами до того, как они попадут в ваши разработки. По мере того, как мы обнаруживаем новые виды атак и проблемы с безопасностью, Sonatype продолжает обеспечивать защиту наших клиентов.

Данные Sonatype об исследованиях безопасности мирового класса в сочетании с нашей технологией автоматического обнаружения вредоносных программ защитят ваших разработчиков, клиентов и цепочку поставок программного обеспечения от заражений». ***(Ax Sharma. Damaging Linux & Mac Malware Bundled within Browserify npm Brandjack Attempt // Sonatype Inc. (https://blog.sonatype.com/damaging-linux-mac-malware-bundled-within-browserify-npm-brandjack-attempt). 13.04.2021).***

***

«Исследователи безопасности из «Лаборатории Касперского» обнаружили вредоносное ПО, встроенное в официальное приложение APKPure популярного стороннего магазина программ для Android, который представляет собой альтернативу официальному магазину Google Play Store.

Вредоносное ПО было встроено в рекламный SDK, входящий в состав APKPure версии 3.7.18. По словам экспертов, вредонос является вариантом трояна Triada, способным рассылать пользователям зараженных устройств рекламный спам, оформлять платные подписки и устанавливать другие вредоносные программы.

«Выявленный вредоносный код, внедренный в APKPure, работает следующим образом — при запуске приложения полезная нагрузка расшифровывается и запускается. Затем вредонос собирает информацию о пользовательском устройстве и отправляет ее на C&C сервер», — пояснили специалисты.

В зависимости от инструкций оператора и схемы монетизации (реклама или плата за установку), ПО способно показывать рекламу каждый раз после разблокирования Android-устройства, повторно открывать web-страницы с рекламой, нажимать на объявления для оформления платных подписок и устанавливать другие полезные данные или потенциально вредоносное программное обеспечение без согласия пользователей.

Хотя официальная статистика количества загрузок приложения APKPure недоступна, специалисты «Лаборатории Касперского» утверждают, что в настоящее время вредоносное ПО было заблокировано на устройствах 9380 Android-пользователей.

Эксперты сообщили разработчикам APKPure о своих находках, и вскоре была выпущена версия APKPure 3.17.19 без вредоносного кода». ***(В приложении APKPure обнаружено вредоносное ПО // SecurityLab.ru (https://www.securitylab.ru/news/518750.php). 12.04.2021).***

***

«TunnelSnake, кампания кибершпионажа, которая, по оценкам специалистов, проводится с 2019 г. и направлена на дипломатические представительства в Азии и Африке, использует ранее неизвестный руткит. Зловред Moriya позволяет совершать практически любые действия в операционной системе, проникать в сетевой трафик и маскировать вредоносные команды, отправляемые на зараженные устройства. С его помощью злоумышленники несколько месяцев тайно контролировали сети жертв.

Эксперты «Лаборатории Касперского» начали расследование, когда получили от защитных продуктов уведомления об обнаружении уникального руткита внутри сетей компаний-жертв. Он умеет скрываться особенно хорошо благодаря двум особенностям.

Во-первых, руткит проникает в сетевые пакеты и проверяет их из пространства адресов ядра Windows – той области памяти, где обычно работает только привилегированный и доверенный код. Это позволяло зловреду отправлять уникальные вредоносные пакеты до их обработки сетевым стеком операционной системы и, как следствие, избегать детектирования защитными решениями. Во-вторых, руткиту не приходилось обращаться к серверу за командами, как это обычно происходит с бэкдорами. Он получал команды в специально промаркированных пакетах, которые приходили в общем потоке сетевого трафика. Это значит, что злоумышленникам не требовалось создавать и поддерживать командно-контрольную инфраструктуру. Кроме того, это позволяло им тщательно скрывать следы присутствия в системе.

В большинстве случаев руткит разворачивался путем компрометации уязвимых веб-серверов внутри сетей компаний-жертв. В одном случае атакующие заразили сервер веб-оболочкой China Chopper. Это вредоносный код, который позволяет удаленно контролировать зараженный сервер.

Кроме руткита Moriya, злоумышленники использовали и другие инструменты – новые кастомизированные или ранее использованные китайскоговорящими APT-группами. С их помощью атакующие сканировали устройства в локальной сети, находили новые цели и распространяли вредоносное ПО.

Исследователям неизвестно кто именно стоит за этой атакой. Но, судя по целям и инструментам, это может быть одна из известных китайскоговорящих групп. Также была обнаружена более старая версию Moriya, использовавшаяся в отдельной атаке 2018 г. Значит, группа, которая стоит за этой кампанией, активна как минимум с того времени. Выбор целей и инструментов позволяет

предположить, что ее цель – шпионаж». ***(Кампания кибершпионажа использовала ранее неизвестный руткит // Компьютерное Обозрение (https://ko.com.ua/kampaniya_kibershpionazha_ispolzovala_ranee_neizvestnyj_rutkit_137069). 16.04.2021).***

***

«Примерно один миллион компьютеров избавляется от вредоносного ПО Emotet после того, как правоохранительные органы предоставили им обновление, которое должно было запустить процесс удаления 25 апреля.

Одна из самых распространенных угроз за последние полвека, Emotet впервые появилась в 2014 году как банковский троянец, но превратилась в загрузчик вредоносного ПО, который использовался многими киберпреступниками для распространения различных полезных нагрузок.

Некоторые из наиболее известных семейств вредоносных программ, распространяемых через Emotet включают TrickBot, RYUK, и QakBot банковских троянов, но и многие другие тоже полагались на массивной сети около одного миллиона зараженных машин для доставки вредоносных файлов.

В январе 2021 года власти объявили, что им удалось захватить серверы Emotet и нарушить работу его инфраструктуры, что привело к остановке работы ботнета.

В то же время голландская полиция начала обновлять зараженные машины, чтобы изолировать заражение. В обновление также было включено несколько строк кода, чтобы вредоносная программа автоматически удалилась 25 апреля.

После запуска команда удаления очищает раздел реестра Windows, который позволяет модулям Emotet запускаться автоматически, а также останавливает и удаляет связанные службы, но не удаляет другие файлы и не стирает дополнительные вредоносные программы, которые могли быть установлены через ботнет.

Кончина Emotet оставляет за собой пустоту, которую, как ожидается, попытаются заполнить другие бот-сети, и исследователи безопасности уже наблюдали рост активности, связанной с вариантами вредоносного ПО BazarCall и IcedID.

«Хотя уничтожение Emotet - большая победа для всех, кроме киберпреступников, попытки заменить его вредоносным ПО, таким как BazarCall и IcedID, демонстрируют, что киберпреступные группы становятся все более организованными, амбициозными и профессиональными. Это почти наверняка останется неизменным и в будущем; На Emotet проблема не заканчивается», - отмечает компания Digital Shadows, занимающаяся защитой от цифровых рисков». ***(Ionut Arghire. Uninstall Command Completes Emotet Botnet Cleanup Operation // Wired Business Media (https://www.securityweek.com/uninstall-command-completes-emotet-botnet-cleanup-operation). 26.04.2021).***

***

«Злоумышленник, говорящий по-китайски, применил новый бэкдор в многочисленных операциях по кибершпионажу, которые длились около двух лет и нацелены на военные организации из Юго-Восточной Азии.

В течение как минимум десяти лет хакерская группа, известная как Naikon, активно шпионила за организациями в странах Южно-Китайского моря, включая Филиппины, Малайзию, Индонезию, Сингапур и Таиланд, по крайней мере, десять лет, начиная с 2010 года.

Naikon, вероятно, является спонсируемым государством субъектом угрозы, связанным с Китаем, в основном известным тем, что сосредоточивает свои усилия на громких организациях, включая правительственные учреждения и военные организации.

Бэкдор, используемый для постоянного резервного копирования после обнаружения

Согласно исследованию, опубликованному сегодня исследователями безопасности из Cyber Threat Intelligence Lab Bitdefender, во время своих атак Naikon злоупотреблял легальным программным обеспечением, чтобы загрузить второстепенное вредоносное ПО, получившее название Nebulae, которое, вероятно, использовалось для достижения устойчивости.

Nebulae предоставляет дополнительные возможности, позволяющие злоумышленникам собирать системную информацию, манипулировать файлами и папками, загружать файлы с командно-управляющего сервера, а также выполнять, перечислять или завершать процессы на скомпрометированных устройствах.

Вредоносная программа также предназначена для обеспечения устойчивости путем добавления нового раздела реестра для автоматического перезапуска при перезапуске системы после входа в систему.

«Данные, которые мы получили до сих пор, почти ничего не говорят о роли туманностей в этой операции, но наличие механизма сохранения может означать, что он используется в качестве резервной точки доступа к жертве в случае негативного сценария для участников», - сказал исследователь Bitdefender Виктор Враби.

Бэкдор первой ступени используется как швейцарский армейский нож

В той же серии атак злоумышленники Naikon также доставили вредоносное ПО первого уровня, известное как RainyDay или FoundCore, используемое для развертывания полезных нагрузок второго уровня и инструментов, используемых для различных целей, включая бэкдор Nebulae.

«Используя бэкдор RainyDay, актеры выполнили разведку, загрузили свои инструменты обратного прокси и сканеры, выполнили инструменты сброса пароля, выполнили боковое перемещение, добились устойчивости, и все это для компрометации сети жертв и получения интересующей информации», - сказал Враби. добавлен [PDF].

Помимо развертывания дополнительных полезных нагрузок в скомпрометированных системах, злоумышленники также могут отправлять команды RainyDay по TCP или HTTP для управления службами, доступа к командной оболочке, удаления вредоносного ПО, снятия и сбора снимков экрана, а также манипулирования, загрузки или выгрузки файлов.

Во время атак, наблюдавшихся в период с июня 2019 года по март 2021 года, Naikon удалял вредоносные полезные нагрузки с помощью уязвимостей боковой загрузки и перехвата DLL, влияя на:

Сервисы Sandboxie COM (BITS) (SANDBOXIE LTD)

Средство поиска элементов Outlook (корпорация Microsoft)

Свойства задачи сканирования по требованию VirusScan (McAfee, Inc.)

Мобильное всплывающее приложение (Quick Heal Technologies (P) Ltd.)

ARO 2012 Учебное пособие

Bitdefender с уверенностью приписал эту операцию злоумышленнику Naikon, основанному на серверах управления и вредоносных данных, принадлежащих семейству вредоносных программ-загрузчиков Aria-Body, которые использовались в прошлых операциях группы». ***(Sergiu Gatlan. Cyberspies target military organizations with new Nebulae backdoor // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/cyberspies-target-military-organizations-with-new-nebulae-backdoor/). 28.04.2021).***

***

«Хакеры, подозреваемые в работе на правительство Китая, использовали новое вредоносное ПО под названием PortDoor для проникновения в системы инженерной компании, проектирующей подводные лодки для ВМФ России.

Они использовали целевое фишинговое письмо, специально созданное для того, чтобы вынудить генерального директора компании открыть вредоносный документ.

Конкретный таргетинг

Злоумышленник нацелился на Центральное конструкторское бюро морской техники «Рубин» в Санкт-Петербурге, оборонного подрядчика, спроектировавшего большую часть российских атомных подводных лодок.

Бэкдор был доставлен в виде документа в формате RTF, прикрепленного к электронному письму, адресованному генеральному директору компании Игорю В. Вильниту.

Исследователи угроз Cybereason Nocturnus обнаружили, что злоумышленник заманил получателя открыть вредоносный документ с общим описанием автономного подводного аппарата.

Копнув глубже, исследователи обнаружили, что файл RTF был превращен в оружие с помощью RoyalRoad, инструмента для создания вредоносных документов для использования множества уязвимостей в Microsoft Equation Editor.

В прошлом использование RoyalRoad было связано с несколькими злоумышленниками, работающими от имени правительства Китая, такими как Tick, Tonto Team, TA428, Goblin Panda, Rancor, Naikon.

При запуске документ RTF отбрасывает бэкдор PortDoor в папке автозагрузки Microsoft Word, маскируя его как файл надстройки, «winlog.wll».

Согласно анализу Cybereason, PortDoor представляет собой полноценный бэкдор с расширенным списком функций, которые делают его подходящим для множества задач:

Занимаюсь разведкой
Профилирование систем-жертв
Скачивание полезной нагрузки с управляющего сервера
Повышение привилегий
Разрешение динамического API для избежания статического обнаружения
Однобайтовое шифрование XOR (конфиденциальные данные, конфигурация)
Кража данных с шифрованием AES

Сегодня в техническом отчете Cybereason Nocturnus Team описываются функциональные возможности вредоносной программы и приводятся индикаторы компрометации, которые помогают организациям защититься от нее.

Исследователи отнесли PortDoor к группе хакеров, спонсируемой Китаем, на основании сходства в тактике, методах и процедурах с другими связанными с Китаем участниками угроз.

На основе работы с исследователем безопасности nao_sec, Cybereason был в состоянии определить, что вредоносный RTF документ был создан с RoaylRoad v7 с кодировкой заголовка, связанной с операциями с Тонто Team (акой CactusPete), Ранкора и TA428.

CactusPete и TA428 известны атаками на организации в Восточной Европе (Россия) и Азии [1, 2, 3, 4]. Кроме того, Cybereason обнаружил лингвистические и визуальные элементы в фишинговом письме PortDoor и документах, которые напоминают приманки в атаках от Tonto Team.

Однако на уровне кода PortDoor не имеет существенного сходства с другими вредоносными программами, используемыми вышеупомянутыми группами, что указывает на то, что это новый бэкдор.

Атрибуция PortDoor в Cybereason не вызывает большой уверенности. Исследователи знают, что за этим вредоносным ПО могут стоять другие группы. Однако текущие данные указывают на злоумышленника китайского происхождения». ***(Ionut Ilascu. Suspected Chinese state hackers target Russian submarine designer // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/suspected-chinese-state-hackers-target-russian-submarine-designer/). 30.04.2021).***

***

Програми-вимагачі

«Недавно Федеральное бюро расследований (ФБР) и Агентство кибербезопасности и безопасности инфраструктуры (CISA) выпустили консультативное предупреждение о недавнем росте числа программ-вымогателей, нацеленных на высшие учебные заведения и школы K-12. Киберпреступники запрашивают платежи в обмен на расшифровку данных, а также угрожают продать личную информацию (например, SSN).

В информационном бюллетене описываются технические детали и индикаторы взлома, в том числе то, что атаки программ-вымогателей PYSA получают несанкционированный доступ к сетям образовательных учреждений

путем компрометации учетных данных и / или с помощью фишинговых писем. Киберпреступники проводят сетевую разведку, устанавливают инструменты с открытым исходным кодом, деактивируют антивирусные возможности в сети, а затем развертывают программы-вымогатели. Киберпреступники вывозят файлы из учреждения и шифруют подключенные устройства и данные, что делает важные файлы, базы данных, виртуальные машины, резервные копии и приложения недоступными для пользователей.

Киберпреступники вывозят записи о занятости, информацию о налогах на заработную плату и другие данные, которые могут быть использованы для вымогательства у учебных заведений с целью выплаты выкупа. Похищенные данные могут быть загружены в облачное хранилище и сервис обмена файлами.

ФБР не рекомендует платить выкуп, так как это поощряет и поощряет преступное поведение. Однако ФБР признало, что образовательные учреждения могут решить заплатить выкуп после того, как выяснят, что существуют ограниченные возможности. ФБР отмечает, что нет никакой гарантии, что выплата выкупа приведет к возврату данных.

ФБР предлагает образовательным учреждениям принять меры по смягчению последствий, в том числе:

Регулярное резервное копирование данных, воздушный зазор и защита паролем резервных копий в автономном режиме. Убедитесь, что копии критически важных данных недоступны для изменения или удаления из системы, в которой они находятся.

Реализуйте сегментацию сети.

Реализуйте план восстановления, чтобы поддерживать и хранить несколько копий конфиденциальных или конфиденциальных данных и серверов в физически отдельном, сегментированном, безопасном месте (например, на жестком диске, устройстве хранения, облаке).

Устанавливайте обновления / патчи для операционных систем, программного обеспечения и микропрограмм сразу после их выпуска.

По возможности используйте многофакторную аутентификацию.

Регулярно меняйте пароли к сетевым системам и учетным записям и избегайте повторного использования паролей для разных учетных записей. Установите максимально короткие приемлемые сроки для смены пароля.

Отключите неиспользуемые порты удаленного доступа / RDP и отслеживайте журналы удаленного доступа / RDP.

Аудит учетных записей пользователей с административными привилегиями и настройка контроля доступа с минимальными привилегиями.

Устанавливайте и регулярно обновляйте антивирусное и антивирусное программное обеспечение на всех хостах.

Используйте только безопасные сети и избегайте общедоступных сетей Wi-Fi. Рассмотрите возможность установки и использования VPN.

Рассмотрите возможность добавления баннера электронной почты к сообщениям, поступающим не из вашей организации.

Отключить гиперссылки в полученных письмах.

Сосредоточьтесь на осведомленности и обучении. Предоставьте пользователям обучение принципам и методам информационной безопасности, а также общим возникающим рискам и уязвимостям кибербезопасности (например, программам-вымогателям и фишинговым атакам).» ***(Meghan C. O'Connor. FBI Issues Warning of Increased Ransomware Targeting Educational Institutions // Quarles & Brady LLP (https://www.quarles.com/publications/fbi-issues-warning-of-increased-ransomware-targeting-educational-institutions/). 08.04.2021).***

***

«Касперский предупреждает, что операторы программ-вымогателей Cring используют старую уязвимость обхода пути в веб-портале FortiOS SSL VPN для получения доступа к корпоративным сетям.

В начале 2021 года было замечено, что злоумышленники, стоящие за вымогателем Cring, совершали многочисленные атаки на европейские промышленные предприятия, вынуждая как минимум одну организацию закрыть производственную площадку.

Первоначальный вектор атаки позже был идентифицирован как CVE-2018-13379, уязвимость веб-портала FortiOS SSL VPN, которая могла позволить злоумышленникам, не прошедшим проверку подлинности, загрузить системные файлы FortiOS.

Уязвимость обхода каталогов может быть использована для извлечения файла сеанса VPN-шлюза, что позволяет злоумышленникам, не прошедшим проверку подлинности, получить доступ к именам пользователей и паролям в виде открытого текста.

Атаки, обнаруженные «Лабораторией Касперского», начались с тестовых подключений к VPN-шлюзу для проверки версии программного обеспечения на целевых устройствах, после чего через несколько дней последовала основная фаза атаки.

«Злоумышленники могли сами идентифицировать уязвимое устройство, просканировав IP-адреса. В качестве альтернативы они могли купить готовый список, содержащий IP-адреса уязвимых устройств Fortigate VPN Gateway», - отмечает Касперский.

Получив первоначальный доступ к корпоративной сети, злоумышленники развернули утилиты сбора учетных данных, которые позволили им скомпрометировать учетную запись администратора домена. Затем они развернули бэкдор Cobalt Strike, чтобы взять под контроль зараженные системы, а затем и программу-вымогатель Cring.

«Различные детали атаки указывают на то, что злоумышленники тщательно проанализировали инфраструктуру атакуемой организации и подготовили свою собственную инфраструктуру и набор инструментов на основе информации, собранной на этапе разведки», - говорит Касперский.

В мае 2019 года Fortinet выпустила уведомление, чтобы проинформировать клиентов о доступности исправлений для CVE-2018-13379, однако многие системы остаются не исправленными, и злоумышленники продолжают использовать это состояние фактов в своих интересах.

Фактически, ФБР и CISA выпустили на прошлой неделе предупреждение, чтобы предупредить правительственные, коммерческие и технологические организации об атаках, направленных на множественные уязвимости в FortiOS. Fortinet также в очередной раз призвала клиентов применять доступные патчи, чтобы оставаться защищенными от атак.

Помимо обеспечения актуальности своего шлюза SSL VPN, организациям рекомендуется изменить политику активного каталога, используя принцип наименьших привилегий, ограничить доступ к VPN, поддерживать резервные копии систем и периодически проверять целостность резервных копий». ***(Ionut Arghire. Cring Ransomware Targets Industrial Organizations // Wired Business Media (https://www.securityweek.com/cring-ransomware-targets-industrial-organizations). 08.04.2021).***

***

«Глобальная эпидемия цифрового вымогательства, известная как программы-вымогатели, наносит ущерб местным органам власти, больницам, школьным округам и предприятиям, шифруя их файлы данных до тех пор, пока они не заплатят. Правоохранительные органы были бессильны остановить это.

Одна важная причина: по мнению исследователей в области безопасности, правоохранительных органов США, а теперь и администрации Байдена, в рэкетах-вымогателях преобладают русскоязычные киберпреступники, которых прикрывают - а иногда и используют - российские спецслужбы.

В четверг, когда США ввели санкции против России за злонамеренные действия, включая взлом при поддержке государства, министерство финансов заявило, что российская разведка способствовала атакам программ-вымогателей, культивируя и кооптируя преступных хакеров и давая им безопасную гавань. Поскольку ущерб от программ-вымогателей теперь исчисляется десятками миллиардов долларов, бывший кибер-глава британской разведки Маркус Уиллетт недавно счел это бедствие, «возможно, более опасным в стратегическом плане, чем государственный кибершпионаж».

Ценность защиты Кремля не теряется для самих киберпреступников. Ранее в этом году русскоязычный форум в даркнете загорелся критикой поставщика программ-вымогателей, известного только как «Bugatti», чья банда была поймана в редких случаях укуса США и Европола. Собранные плакаты обвиняли его в том, что он призывал к разгрому с технической небрежностью и вербовал нероссийские аффилированные лица, которые могли быть доносчиками или тайными полицейскими.

Хуже всего то, что, по мнению одного из давних участников форума, Bugatti позволила западным властям захватить серверы вымогателей, которые вместо этого могли быть укрыты в России. «Матушка Россия поможет», - написал этот человек. «Любите свою страну, и с вами ничего не случится». Разговор был записан охранной фирмой Advanced Intelligence, которая поделилась им с Associated Press.

«Как и почти любая крупная отрасль в России, (киберпреступники) работают с молчаливым, а иногда и с явным согласием служб безопасности», - сказал Майкл

ван Ландингем, бывший аналитик ЦРУ, руководящий консалтинговой компанией Active Measures LLC.

У российских властей есть простое правило, - сказал Карен Казарян, генеральный директор Института интернет-исследований в Москве, который поддерживается индустрией программного обеспечения: «Просто никогда не работайте против своей страны и бизнеса в этой стране. Если украдете что-нибудь у американцев, ничего страшного».

В отличие от Северной Кореи, нет никаких указаний на то, что правительство России напрямую извлекает выгоду из преступлений, связанных с использованием программ-вымогателей, хотя президент России Владимир Путин может счесть причиненный ущерб стратегическим бонусом.

По данным фирмы Emsisoft, занимающейся кибербезопасностью, только в США в прошлом году программа-вымогатель поразила более сотни федеральных, государственных и муниципальных учреждений, более 500 больниц и других медицинских центров, около 1680 школ, колледжей и университетов и сотни предприятий.

Ущерб в государственном секторе измеряется только измененным маршрутом скорой помощи, отложенным лечением рака, прерванным сбором муниципальных счетов, отмененными занятиями и ростом расходов на страхование - все это во время самого серьезного кризиса общественного здравоохранения за более чем столетие.

Идея этих атак проста: злоумышленники внедряют вредоносное программное обеспечение для шифрования данных в компьютерные сети, используют его для «похищения» файлов данных организации, а затем требуют огромных платежей, которые сейчас достигают 50 миллионов долларов, для их восстановления. Последний поворот: если жертвы не заплатят, преступники могут опубликовать свои нешифрованные данные в открытом Интернете.

В последние месяцы правоохранительные органы США работали с партнерами, включая Украину и Болгарию, над взломом этих сетей. Но поскольку криминальные вдохновители недосягаемы, такие операции, как правило, не более чем чушь.

По словам заместителя помощника генерального прокурора США Адама Хики, в сговоре между преступниками и правительством нет ничего нового для России, отметив, что киберпреступность может служить хорошим прикрытием для шпионажа.

По словам Казаряна, еще в 1990-х годах российская разведка часто нанимала для этой цели хакеров. Теперь, по его словам, преступники-вымогатели с такой же вероятностью подрабатывают государственных хакеров.

Кремль иногда вербует арестованных хакеров-преступников, предлагая им выбор между тюрьмой и работой на государство, сказал Дмитрий Альперович, бывший технический директор компании Crowdstrike, занимающейся кибербезопасностью. По его словам, иногда хакеры используют одни и те же компьютерные системы для санкционированного государством взлома и для киберпреступности в нерабочее время для личного обогащения. Они могут даже смешивать государство с личным бизнесом.

Именно это произошло во время взлома Yahoo в 2014 году, в результате которого было скомпрометировано более 500 миллионов учетных записей пользователей, в том числе предположительно российских журналистов и государственных чиновников США и России. В результате расследования, проведенного в США, в 2017 году было предъявлено обвинение четырем мужчинам, в том числе двум сотрудникам службы безопасности ФСБ России - преемницы КГБ. Один из них, Дмитрий Докучаев, работал в том же управлении ФСБ, которое сотрудничает с ФБР по компьютерным преступлениям. Другой обвиняемый, Алексей Белан, предположительно использовал взлом в личных целях.

Представитель посольства России отказался отвечать на вопросы о предполагаемых связях его правительства с преступниками-вымогателями и предполагаемой причастности государственных служащих к киберпреступности. «Мы не комментируем обвинительные заключения или слухи», - сказал Антон Азизов, заместитель пресс-атташе в Вашингтоне.

Доказать связь между российским государством и бандами вымогателей непросто. Преступники прячутся за псевдонимами и периодически меняют названия своих вредоносных программ, чтобы запутать западные правоохранительные органы.

Но по крайней мере один поставщик программ-вымогателей был связан с Кремлем. 33-летний Максим Якубец наиболее известен как соруководитель кибергруппы, которая дерзко называет себя Evil Corp. Якубец, уроженец Украины, ведет яркий образ жизни. Он водит индивидуальный суперкар Lamborghini с персонализированным номерным знаком, что переводится как «вор». по данным Национального агентства по борьбе с преступностью Великобритании.

Якубец начал работать в ФСБ в 2017 году, отвечая за проекты, включая «получение конфиденциальных документов с помощью кибер-средств и проведение кибероперациий от его имени», согласно обвинительному заключению США от декабря 2019 года. В то же время министерство финансов США ввело санкции в отношении Якубца и предложило вознаграждение в размере 5 миллионов долларов за информацию, ведущую к его поимке. В нем говорилось, что он, как известно, «находился в процессе получения от ФСБ лицензии на работу с российской секретной информацией».

В обвинительном заключении Evil Corp. было обвинено в разработке и распространении программ-вымогателей, использовавшихся для кражи не менее 100 миллионов долларов в более чем 40 странах за предыдущее десятилетие, включая платежные ведомости, похищенные из городов в центре Америки.

К тому времени, когда Якубцу было предъявлено обвинение, Evil Corp. стала крупным поставщиком программ-вымогателей, говорят исследователи в области безопасности. К маю 2020 года банда распространяла штамм вымогателя, который использовался для атаки восьми компаний из списка Fortune 500, включая производителя GPS-устройств Garmin, чья сеть была отключена в течение нескольких дней после атаки, согласно Advanced Intelligence.

Якубец остается на свободе. Однако другой россиянин, который в настоящее время находится в тюрьме во Франции, может дать больше информации о сделках

киберпреступников и российского государства. Александр Винник был осужден за отмывание 160 миллионов долларов преступных доходов через криптовалютную биржу BTC-e. В обвинительном заключении США от 2017 года говорилось, что «некоторые из крупнейших известных поставщиков программ-вымогателей» фактически использовали их для отмывания 4 миллиардов долларов. Но Винник не может быть экстрадирован до тех пор, пока в 2024 году он не завершит свой 5-летний тюремный срок во Франции.

Тем не менее, исследование, проведенное в 2018 году независимым аналитическим центром Third Way, показало, что шансы на успешное преследование авторов кибератак на цели в США - программы-вымогатели и кражи онлайн-банков - самые дорогостоящие - не превышают трех из тысячи. Эксперты говорят, что эти шансы увеличились.

Многие аналитики считают, что санкции, введенные на этой неделе, являются серьезным сигналом, но вряд ли они остановят Путина, если финансовое положение не ударит по его дому.

Для этого может потребоваться такая масштабная международная координация, которая последовала за террористическими атаками 11 сентября. Например, страны-союзники могут идентифицировать банковские учреждения, которые отмывают доходы от программ-вымогателей, и отрезать их от мирового финансового сообщества…». ***(How the Kremlin Provides a Safe Harbor for Ransomware // Wired Business Media (https://www.securityweek.com/how-kremlin-provides-safe-harbor-ransomware). 16.04.2021).***

***

«Компания, которая стала жертвой атаки программы-вымогателя и заплатила киберпреступникам миллионы за ключ дешифрования для восстановления их сети, через две недели стала жертвой той же самой банды вымогателей, не сумев выяснить, почему атака вообще могла произойти.

Поучительная история подробно описана Национальным центром кибербезопасности Великобритании (NCSC) в сообщении блога о росте числа программ-вымогателей.

Неназванная компания стала жертвой атаки программы-вымогателя и заплатила миллионы в биткойнах, чтобы восстановить сеть и получить файлы.

Однако компания просто оставила все как есть, не сумев проанализировать, как киберпреступники проникли в сеть - то, что вернулось, чтобы преследовать их, когда та же банда вымогателей заразила сеть той же программой-вымогателем менее чем через две недели. В итоге компания заплатила выкуп во второй раз.

«Мы слышали об одной организации, которая заплатила выкуп (немногим менее 6,5 миллионов фунтов стерлингов при сегодняшнем обменном курсе) и восстановила свои файлы (с помощью поставляемого дешифратора), не прилагая никаких усилий для выявления основной причины и защиты своей сети. Менее чем две недели спустя тот же злоумышленник снова атаковал сеть жертвы, используя тот же механизм, что и раньше, и повторно развернул свою программу-вымогатель. Жертва почувствовала, что у нее нет другого выбора, кроме как снова заплатить выкуп», - говорится в блоге NCSC.

NCSC детализировал этот инцидент как урок для других организаций - и урок состоит в том, что если вы станете жертвой атаки вымогателя, узнайте, как киберпреступники могли незаметно внедриться в сеть до того, как была запущена полезная нагрузка вымогателя.

«Для большинства жертв, которые обращаются к NCSC, их первоочередной задачей является - по понятным причинам - вернуть свои данные и обеспечить возобновление работы своего бизнеса. Однако настоящая проблема заключается в том, что программы-вымогатели часто являются лишь видимым симптомом более серьезного сетевого вторжения. это могло сохраняться в течение нескольких дней, а возможно и дольше», - говорится в сообщении в блоге технического руководителя NCSC по управлению инцидентами.

Чтобы установить программу-вымогатель, киберпреступники могли получить бэкдорный доступ к сети - возможно, через предыдущее вторжение вредоносного ПО - а также имея права администратора или другие учетные данные.

Если у злоумышленников есть это, они могут легко развернуть другую атаку, если захотят - и это сделали, в примере, подробно описанном выше, поскольку жертва не исследовала, как была взломана их сеть.

Таким образом, изучение сети после инцидента с программой-вымогателем и определение того, как вредоносная программа смогла проникнуть в сеть, а также оставаться незамеченной так долго, - это то, что все организации, ставшие жертвами вымогателя, должны учитывать наряду с восстановлением сети - или, предпочтительно, до они даже думают о восстановлении сети.

Некоторые могут подумать, что уплата выкупа преступникам будет самым быстрым и наиболее экономичным способом восстановления сети, но это также случается редко. Потому что не только выплачивается выкуп, который может стоить миллионы, но и анализ после события и восстановление поврежденной сети также стоит больших сумм.

И, как отмечает NCSC, попадание в жертву атаки программ-вымогателей часто приводит к длительному периоду сбоев, прежде чем операции станут похожими на что-то нормальное.

«Восстановление после инцидента с программой-вымогателем редко бывает быстрым процессом. Расследование, восстановление системы и восстановление данных часто требуют нескольких недель работы», - говорится в сообщении.

Лучший способ избежать всего этого - убедиться, что ваша сеть защищена от кибератак, в первую очередь, сделав такие вещи, как обновление операционных систем и исправлений безопасности, а также применение многофакторной аутентификации в сети.

Также рекомендуется, чтобы организации регулярно создавали резервные копии своих сетей и хранили эти резервные копии в автономном режиме, чтобы в случае успешной атаки вымогателей сеть можно было восстановить с наименьшими возможными сбоями». ***(Danny Palmer. Ransomware: A company paid millions to get their data back, but forgot to do one thing. So the hackers came back again // ZDNet (https://www.zdnet.com/article/ransomware-this-is-the-first-thing-you-should-think-about-if-you-fall-victim-to-an-attack/). 05.04.2021).***

***

«Недавние атаки операторов программ-вымогателей Ryuk показывают, что у злоумышленников появилось новое предпочтение, когда дело доходит до получения первоначального доступа к сети жертвы.

Тенденция, наблюдаемая в атаках в этом году, выявляет склонность к атакам на хосты с подключениями к удаленным рабочим столам, доступными в общедоступном Интернете.

Более того, использование целевых фишинговых писем для доставки вредоносного ПО по-прежнему является предпочтительным исходным вектором заражения для злоумышленников.

Новая тенденция первичного заражения

Исследователи в области безопасности из бутика анализа угроз Advanced Intelligence (AdvIntel) отметили, что атаки программ-вымогателей Ryuk в этом году чаще основывались на компрометации открытых соединений RDP, чтобы получить первоначальную точку опоры в целевой сети.

Злоумышленники проводили «крупномасштабные атаки методом грубой силы и распыления паролей на открытые хосты RDP», чтобы скомпрометировать учетные данные пользователей.

Другим вектором первоначального взлома был целевой фишинг и использование кампании BazaCall для распространения вредоносного ПО через злонамеренные центры обработки вызовов, которые предназначались для корпоративных пользователей и перенаправляли их к документам Excel, вооруженным оружием.

Исследователи AdvIntel утверждают, что злоумышленники Ryuk провели разведку жертвы в два этапа. Один раз, чтобы определить ценные ресурсы в скомпрометированном домене (общие сетевые ресурсы, пользователи, организационные единицы Active Directory).

Во второй раз цель состоит в том, чтобы найти информацию о доходах компании, чтобы установить сумму выкупа, которую жертва может позволить себе заплатить за восстановление систем.

Для перечисления информации об активном каталоге операторы программ-вымогателей Ryuk полагаются на испытанный и проверенный AdFind (инструмент запросов AD) и инструмент после эксплуатации Bloodhound, который исследует отношения в домене Active Directory (AD) для поиска путей атаки.

Получение финансовых сведений о жертве зависит от данных из открытых источников. AdvIntel сообщает, что субъекты ищут в таких сервисах, как ZoomInfo, информацию о недавних слияниях и поглощениях компании, а также другие детали, которые могут повысить прибыльность атаки.

Дополнительная разведка выполняется с помощью инструмента пост-эксплуатации Cobalt Strike, который стал стандартом для большинства операций с программами-вымогателями и сканирования, которые выявляют продукты безопасности, такие как антивирус и ответ на обнаружение конечных точек (EDR), защищающие сеть.

Новые техники

В Исследователи говорят, что актер занимается другими киберпреступниками, чтобы узнать о защиты в сети они нападают, чтобы найти способ, чтобы отключить их.

Среди новых методов, которые исследователи увидели в атаках программ-вымогателей Ryuk, было использование KeeThief, инструмента с открытым исходным кодом для извлечения учетных данных из диспетчера паролей KeePass.

KeeThief извлекает ключевой материал (например, мастер-пароль, ключевой файл) из памяти запущенного процесса KeePass с разблокированной базой данных.

Виталий Кремез, генеральный директор AdvIntel, сообщил BleepingComputer, что злоумышленники использовали KeeThief для обхода EDR и других средств защиты путем кражи учетных данных местного ИТ-администратора, имеющего доступ к программному обеспечению EDR.

Еще одна тактика заключалась в развертывании портативной версии Notepad ++ для запуска сценариев PowerShell в системах с ограничением выполнения PowerShell, говорит Кремез.

По данным AdvIntel, атаки программ-вымогателей Ryuk в этом году используют две уязвимости для увеличения разрешений на скомпрометированной машине. Оба недостатка старше и для них доступны исправления:

CVE-2018-8453 - повышение привилегий с высоким уровнем серьезности (7,8 / 10) в Windows 7–10 и Windows Server 2008–2016, что позволяет запускать произвольное ядро с разрешениями на чтение / запись, поскольку компонент Win32k не может должным образом обрабатывать объекты в памяти

CVE-2019-1069 - повышение привилегий с высокой степенью серьезности (7,8 / 10) в Windows 10, Windows Server 2016 и 2019 из-за того, как служба планировщика заданий проверяет определенные файловые операции, что делает возможной атаку жесткой ссылки

Еще одно наблюдение от AdvIntel заключается в том, что недавняя атака программы-вымогателя Ryuk использовала инструмент проникновения CrackMapExec с открытым исходным кодом для извлечения учетных данных администратора и перемещения по сети жертвы.

Исследователи рекомендуют организациям следующие шаги по снижению рисков:

обнаруживать использование Mimikatz и выполнение PsExec в сети

оповещения о наличии AdFind, Bloodhound и LaZagne в сети

убедитесь, что операционные системы и программное обеспечение имеют последние исправления безопасности

реализовать многофакторную аутентификацию для доступа RDP

сегментация сети и элементы управления для проверки трафика SMB и NTLM

использовать принцип наименьших привилегий и рутинные проверки прав доступа к аккаунту

Регулярный обзор Регулярно проверяйте разрешения учетной записи, чтобы предотвратить сползание привилегий и придерживаться принципа наименьших привилегий

регулярный просмотр объектов групповой политики и сценариев входа в систему

системы исправлений против CVE-2018-8453 и CVE-2019-1069

Рюк давно занимается программами-вымогателями и известен как жесткий переговорщик. По оценкам, они собрали выкуп не менее 150 миллионов долларов, при этом одна жертва в конечном итоге заплатила 34 миллиона долларов за восстановление своих систем.

Учитывая эти цифры, логично предположить, что актер переключился на новую тактику, приемы и процедуры, чтобы оставаться впереди всех и поддерживать прибыльный бизнес с программами-вымогателями». ***(Ionut Ilascu. Ryuk ransomware operation updates hacking techniques // Bleeping Computer (https://www.bleepingcomputer.com/news/security/ryuk-ransomware-operation-updates-hacking-techniques/). 17.04.2021).***

***

«Атака программы-вымогателя на компанию Bakker Logistiek, занимающуюся складированием и транспортировкой, вызвала нехватку сыра в голландских супермаркетах.

Bakker Logistiek - один из крупнейших поставщиков логистических услуг в Нидерландах, предлагающий складирование с кондиционированием воздуха и транспортировку продуктов питания для голландских супермаркетов.

На прошлой неделе компания Bakker Logistiek подверглась атаке программы-вымогателя, которая зашифровала устройства в их сети и нарушила операции по транспортировке и доставке еды.

«Мы больше не могли получать заказы от клиентов», - сказал NOS директор Bakker Тун Верховен. «А на наших складах мы больше не знали, где находятся продукты. Это очень большие склады, вы не просто ищете поддон. Мы также больше не могли планировать наши перевозки. У нас есть сотни грузовиков, что не было сделано вручную либо».

Этот сбой привел к нехватке некоторых продуктов питания, особенно сыра, в крупнейшей сети супермаркетов Нидерландов Albert Heijn.

Дефицит побудил Альберта Хейна разместить на своем веб-сайте уведомление, предупреждающее покупателей об ограниченной доступности расфасованного сыра.

«Из - за технической неисправности, существует ограниченная доступность на расфасованный сыр. Поставщик логистических услуг работает, чтобы решить проблему как можно быстрее, и быстро восстановить доступность. Приносим извинения за неудобства,» АН размещен на их сайте.

Компания Bakker Logistiek заявила, что может восстановить поврежденные системы из резервных копий, и начала согласовывать действия с клиентами, чтобы снова начать поставки.

Неизвестно, какая банда вымогателей нацелилась на Bakker Logistiek, но Верховен сообщил NOS, что они предполагают, что злоумышленники получили доступ к их системам через недавно обнаруженные уязвимости Microsoft Exchange ProxyLogon…». ***(Lawrence Abrams. Dutch supermarkets run out of cheese after***

ransomware attack // Bleeping Computer (https://www.bleepingcomputer.com/news/security/dutch-supermarkets-run-out-of-cheese-after-ransomware-attack/). 12.04.2021).

***

«Недавнее изменение вымогателя REvil позволяет злоумышленникам автоматизировать шифрование файлов в безопасном режиме после изменения паролей Windows.

В марте мы сообщили о новом режиме шифрования Windows Safe Mode, добавленном в программу-вымогатель REvil / Sodinokibi. Этот режим можно включить с помощью аргумента командной строки -smode, который перезагрузит устройство в безопасном режиме, где оно будет выполнять шифрование файлов.

Считается, что этот режим был добавлен как способ избежать обнаружения программным обеспечением безопасности и выключить программное обеспечение резервного копирования, серверы баз данных или почтовые серверы, чтобы добиться большего успеха при шифровании файлов.

Однако на момент написания нашего отчета программа-вымогатель требовала, чтобы кто-то вручную входил в безопасный режим Windows до начала шифрования, что могло вызвать тревогу.

Новая версия автоматически переводит Windows в безопасный режим.

В конце марта исследователь безопасности R3MRUM обнаружил новый образец вымогателя REvil, который усовершенствовал новый метод шифрования в безопасном режиме, изменив пароль вошедшего в систему пользователя и настроив Windows на автоматический вход при перезагрузке.

В этом новом примере при использовании аргумента -smode программа-вымогатель изменит пароль пользователя на « DTrump4ever».

Затем программа-вымогатель настраивает следующие значения реестра, чтобы Windows автоматически входила в систему с новой информацией учетной записи.

Хотя неизвестно, будут ли новые образцы шифровальщика REvil использовать пароль «DTrump4ever», по крайней мере два образца, загруженные на VirusTotal за последние два дня, продолжают использовать пароль.

Эти изменения показывают, как банды программ-вымогателей постоянно развивают свою тактику для успешного шифрования устройств жертв и принудительного уплаты выкупа.

REvil также недавно предупредил, что они будут выполнять DDoS-атаки на жертв и их деловых партнеров по электронной почте о украденных данных, если выкуп не будет уплачен». ***(Lawrence Abrams. REvil ransomware now changes password to auto-login in Safe Mode // Bleeping Computer (https://www.bleepingcomputer.com/news/security/revil-ransomware-now-changes-password-to-auto-login-in-safe-mode/). 07.04.2021).***

***

«Канадский поставщик решений IoT Sierra Wireless объявила о возобновлении производства на своих производственных площадках,

остановленных после атаки программ-вымогателей, поразивших его внутреннюю сеть и корпоративный веб-сайт 20 марта.

Узнав об атаке, компания наняла услуги «KPMG, одной из ведущих в мире фирм по судебно-медицинским расследованиям и реагированию на киберинциденты, чтобы руководить реагированием и расследованием инцидента Sierra Wireless».

ИТ-специалисты Siera Wireless в настоящее время работают над восстановлением своих внутренних систем после того, как вернули в онлайн свой корпоративный веб-сайт.

Канадская транснациональная компания добавила, что атака программы-вымогателя не повлияла на ее продукты и услуги, ориентированные на клиентов, поскольку затронутые внутренние ИТ-системы разделены.

«Sierra Wireless считает, что воздействие атаки было ограничено внутренними системами Sierra Wireless и корпоративным веб-сайтом, и что ее продукты и услуги связи не пострадали, а продукты и системы ее клиентов не были взломаны во время атаки», - говорится в сообщении компании. сказал.

«На данном этапе расследования атаки с использованием программ-вымогателей компания не ожидает, что в результате атаки потребуются какие-либо исправления безопасности для продуктов или обновления прошивки или программного обеспечения».

"Конфиденциальные" подробности инцидента с программой-вымогателем

Компания не предоставила информацию о том, какая операция вымогателя стояла за атакой или были ли какие-либо данные украдены из скомпрометированных систем до того, как они были зашифрованы в заявлении, опубликованном 25 марта.

После мартовской атаки программы-вымогателя компания также отозвала свой прогноз на первый квартал 2021 года, представленный в прошлом месяце, 23 февраля.

Представитель Sierra Wireless сообщил BleepingComputer, что никаких дополнительных подробностей не разглашается, поскольку «протоколы компании для борьбы с любыми атаками программ-вымогателей» «считаются очень чувствительными и конфиденциальными».

«Безопасность является главным приоритетом, и Sierra Wireless обязуется принимать все необходимые меры для обеспечения высочайшей целостности всех наших систем», - сказал Сэм Кокрейн, финансовый директор Sierra Wireless, отвечающий за ИТ-операции и цепочку поставок.

«По мере продолжения расследования Sierra Wireless обязуется напрямую общаться со всеми затронутыми клиентами или партнерами, которых мы благодарим за их терпение, пока мы работаем с этой ситуацией».

Канадская многонациональная компания со штаб-квартирой в Ричмонде, Британская Колумбия, с центрами исследований и разработок в Северной Америке, Европе и Азии, насчитывает более 1300 сотрудников по всему миру.

Продукты Siera Wireless (включая беспроводные модемы, маршрутизаторы и шлюзы), продаваемые напрямую OEM-производителям, используются в устройствах Интернета вещей и других электронных устройствах, таких как

смартфоны, и во многих отраслях промышленности, включая автомобилестроение и транспорт, энергетику, здравоохранение, промышленность и т.д. инфраструктура, вычисления, сети и безопасность». ***(Sergiu Gatlan. Sierra Wireless resumes production after ransomware attack // Bleeping Computer (https://www.bleepingcomputer.com/news/security/sierra-wireless-resumes-production-after-ransomware-attack/). 04.04.2021).***

***

«Национальный колледж Ирландии (NCI) и Дублинский технологический университет объявили, что атаки программ-вымогателей поражают их ИТ-системы.

NCI в настоящее время работает над восстановлением ИТ-сервисов после того, как в минувшие выходные подверглась атаке программ-вымогателей, в результате чего колледж отключил ИТ-системы.

«NCI в настоящее время испытывает значительные перебои в предоставлении ИТ-услуг, которые повлияли на ряд систем колледжа, включая Moodle, библиотечную службу и текущую студенческую службу MyDetails», колледж объявлено в субботу.

В последующем обновлении после атаки программы-вымогателя 3 апреля преподаватели и сотрудники были уведомлены о том, что ИТ-персонал и внешние поставщики услуг работают над восстановлением служб.

Доступ к ИТ-системам NCI был приостановлен, а здание кампуса в настоящее время закрыто как для студентов, так и для персонала до восстановления ИТ-услуг.

NCI также уведомила об инциденте соответствующие органы, в том числе комиссара по защите данных и Gardaí (национальную полицейскую службу Ирландской Республики.

«Обратите внимание, что все классы, оценки и вводные занятия, запланированные с сегодняшнего вторника 6-го по этот четверг 8-го апреля включительно, были отложены и будут перенесены на более позднюю дату», - говорится в заявлении NCI, опубликованном сегодня.

«Колледж опубликует дополнительную информацию о занятиях и других мероприятиях в пятницу и далее в четверг днем».

Студентам, которые должны были сдать задания на этой неделе, сказали, что «не будут применяться штрафы за просрочку, пока отключение остается на месте».

Кампус Таллахтского технологического университета Дублина (TU Dublin) был поражен атакой программы-вымогателя в четверг утром и затронул как ИТ-системы, так и резервные копии университетских городков.

«Нарушение работы некоторых систем ИКТ в кампусе Таллахта, но доступен безопасный удаленный доступ к ключевым услугам», - говорится в сообщении TU Dublin на веб-сайте университета. «Служба поддержки ICT не может отвечать на запросы, пока исследуются проблемы. Обновления будут отправляться по электронной почте».

Согласно электронному письму, отправленному студентам и полученному DataBreaches, «эта атака не затрагивает какие-либо системы или процессы ИКТ в кампусах Сити и Бланчардстауна».

Студентам также было сказано не использовать какие-либо ИТ-системы кампуса до понедельника, 12 апреля, и избегать обращения к ИТ-персоналу, который в настоящее время работает над восстановлением поврежденных ИТ-систем.

«На этой ранней стадии расследования нет никаких указаний на то, что какие-либо данные, включая личные данные, были отфильтрованы, загружены, скопированы или отредактированы из-за этой атаки», - сказал BleepingComputer представитель Дублинского университета.

«Университет продолжает работать в срочном порядке, чтобы как можно скорее восстановить безопасный доступ студентов и сотрудников ко всем нашим локальным системам ИКТ».

Из других новостей следует отметить, что Университет Брауна, частный исследовательский университет Лиги плюща в США, все еще работает над выводом систем в онлайн после того, как ему пришлось отключить их после кибератаки во вторник.

В прошлом месяце киберотдел Федерального бюро расследований (ФБР) предупредил специалистов по кибербезопасности об увеличении активности программы-вымогателя Pysa, нацеленной на учебные заведения в 12 штатах США и Великобритании.

На данный момент нет информации о бандах вымогателей, стоящих за двумя атаками. Представитель NCI не был доступен для комментариев, когда сегодня с ним связались представители BleepingComputer». ***(Sergiu Gatlan. Ransomware hits TU Dublin and National College of Ireland // Bleeping Computer (https://www.bleepingcomputer.com/news/security/ransomware-hits-tu-dublin-and-national-college-of-ireland/). 06.04.2021).***

***

«Програма-вимагач, яку використовують для кібератак, задіює архіватор 7-Zip для «шифрування» файлів. Надалі за відновлення доступу зловмисники вимагають гроші.

Потрапляючи в систему, шкідливе програмне забезпечення створює захищені паролем архіви 7-Zip розміром – 20МБ, у які «запаковує» файли, що містяться на пристрої. Потерпілі при відкритті текстового файлу, створеного криптолокером «Qlocker», виявляють посилання на ресурс, розміщений у мережі TOR. Далі пропонується ввести персональний ID, який присвоюється пристрою вірусом-вимагачем, та у подальшому отримати електронний гаманець у криптовалюті.

Для дешифрування жертві потрібно ввести пароль, що відомий лише оператору «Qlocker». За відновлення доступу зловмисники вимагають у постраждалих гроші.

Кіберзлочинці використовують критичні вразливості в операційних системах QNAP, а саме CVE-2020-2509 (вразливість дозволяє зловмисникам виконувати довільні команди в компрометованому додатку), CVE-2020-36195 (SQL-ін’єкція в

QNAP Multimedia Console and Media Streaming Add-On)…». ***(Кіберполіція попереджає про масштабну світову кібератаку на пристрої QNAP // Національна поліція (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-poperedzhaje-pro-masshtabnu-svitovu-kiberataku-na-pristroji-QNAP/). 23.04.2021).***

***

«Предполагается, что британская железнодорожная компания Merseyrail подверглась атаке с использованием программ-вымогателей, и виновные в этом мошенники, как сообщается, взломали учетную запись директора Office 365, чтобы отправлять сообщения сотрудникам и журналистам по электронной почте.

Новость о взломе сообщила компания BleepingComputer, получившая одно из таких писем.

Представитель железнодорожного оператора сообщил нам в заявлении: «Недавно компания Merseyrail подверглась кибератаке. Было начато полное расследование и уведомлены соответствующие органы. Это не повлияет на работу наших сервисов, которые будут продолжать работать в соответствии с объявлением».

Сеть Merseyrail охватывает 68 станций вокруг Ливерпуля, Биркенхеда и Саутпорта, простираясь на юг до Честера.

Утверждалось, что ответственной группой была банда Локбита, относительно новая организация. Darktrace считает, что впервые он был замечен в 2019 году и использовал такие инструменты, как PowerShell, для компрометации своих жертв. По подсчетам Darktrace, средний запрос Lockbit на выкуп составлял 40 000 долларов.

Описывая предыдущее заражение одного из своих клиентов, Darktrace сказал: «Атака началась, когда киберпреступник получил доступ к одной привилегированной учетной записи - либо посредством атаки грубой силы на внешнее устройство, как это было замечено в предыдущих атаках программ-вымогателей LockBit., или просто с помощью фишингового сообщения электронной почты».

Компания Sophos провела технический анализ Lockbit еще в 2020 году, отметив, что команда отказывается нацеливаться на жертв из Содружества Независимых Государств (в основном из бывшего Советского Союза). При развертывании он пытается убить процессы Windows, включая продукты от Norton, Symantec, Sophos и Qihoo360, а также пакеты резервного копирования. Он также сохраняется после завершения работы через раздел реестра.

Управление комиссара по информации заявило, что ему известно об атаке программ-вымогателей на компанию Merseyrail, которая была признана самым надежным оператором поездов в Великобритании второй год подряд». ***(Gareth Corfield. Ransomware crooks who broke into Merseyrail used director's email address to brag about it – report // The Register (https://www.theregister.com/2021/04/28/merseyrail_ransomware_claim/). 28.04.2021).***

***

«Целевая группа по программам-вымогателям, общественная коалиция, состоящая из более чем 50 экспертов, поделилась рамками действий по разрушению бизнес-модели программ-вымогателей.

Одна из приоритетных рекомендаций относится к лучшему регулированию сектора криптовалюты, который играет важную роль в сокрытии злоумышленников и превращении атак программ-вымогателей в прибыльное дело.

Приоритетные действия

В опубликованном сегодня документе Институт безопасности и технологий (IST) предоставляет список из 48 действий, которые правительства и лидеры частного сектора могут предпринять для серьезного сдерживания угрозы программ-вымогателей.

В последние годы активность программ-вымогателей постоянно росла, поскольку киберпреступники усилили свои атаки на цели как в частном, так и в государственном секторе (включая здравоохранение и образование).

В прошлом году требования о выкупе составляли в среднем сотни тысяч долларов США, но самые высокие выплаты составляли от 1 до 2 миллионов долларов для некоторых банд вымогателей.

Приоритетные рекомендации:

Скоординированные международные дипломатические и правоохранительные усилия должны упреждающе определять приоритеты программ-вымогателей с помощью комплексной стратегии с ресурсами, включая использование подхода кнута и пряника, чтобы увести национальные государства от предоставления убежища для преступников-вымогателей.

Соединенные Штаты должны подавать пример и проводить устойчивую, агрессивную, общегосударственную кампанию по борьбе с программами-вымогателями, основанную на разведке и координируемую Белым домом. В США это должно включать создание: 1) Межведомственной рабочей группы во главе с Советом национальной безопасности в координации с формирующимся Национальным кибердиректором; 2) внутренняя совместная рабочая группа правительства США по программам-вымогателям; и 3) совместный, частный неформальный центр изучения угроз вымогателей.

Правительствам следует создать фонды киберответа и восстановления для поддержки реагирования на программы-вымогатели и других мероприятий по кибербезопасности; обязать организации сообщать о выплатах выкупа; и потребовать от организаций рассмотреть альтернативы перед осуществлением платежей.

Необходимо разработать скоординированные на международном уровне усилия для разработки четкой, доступной и широко принятой структуры, которая поможет организациям подготовиться к атакам программ-вымогателей и отреагировать на них. В некоторых секторах с ограниченными ресурсами и в более важных секторах для стимулирования внедрения могут потребоваться стимулы (например, компенсация штрафов и финансирование) или регулирование.

Сектор криптовалюты, который способствует преступлениям с использованием программ-вымогателей, следует более строго регулировать. Правительствам следует требовать от бирж криптовалют, крипто-киосков и

внебиржевых торговых «столов» соблюдения существующих законов, в том числе «Знай своего клиента» (KYC), борьбы с отмыванием денег (AML) и борьбой с финансированием терроризма (CFT) законы.

Нужна помощь Конгресса

Некоторые правила, разработанные Целевой группой по программам-вымогателям (RTF), требуют помощи Конгресса для модернизации некоторых законов о кибербезопасности, таких как Закон о совместном использовании информации о кибербезопасности 2015 года и Закон о компьютерном мошенничестве и злоупотреблениях (CFAA).

Изменения должны стимулировать жертв программ-вымогателей анонимно делиться реквизитами платежей программ-вымогателей (адреса криптовалютных кошельков, хэши транзакций, заметки о выкупе).

Они также должны разрешать более широкий набор действий сторонам, имеющим дело с инцидентом с вымогателем, «действуя добросовестно, не опасаясь юридической ответственности».

Рекомендации RTF рассчитаны на долгосрочное воздействие после принятия и, вероятно, улучшат состояние кибербезопасности организаций. Они также могут укрепить сотрудничество между несколькими участниками, стремящимися защитить мир от киберугроз». ***(Ionut Ilascu. Security expert coalition shares actions to disrupt ransomware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/security-expert-coalition-shares-actions-to-disrupt-ransomware/). 29.04.2021).***

***

«Бразильский Tribunal de Justiça do Estado do Rio Grande do Sul вчера подвергся атаке программы-вымогателя REvil, которая зашифровала файлы сотрудников и вынудила суды закрыть их сеть.

Tribunal de Justiça do Estado do Rio Grande do Sul (TJRS) - это судебная система бразильского штата Риу-Гранди-ду-Сул.

Атака началась вчера утром, когда сотрудники внезапно обнаружили, что все их документы и изображения больше не доступны, а на их рабочих столах Windows появились заметки о выкупе.

Вскоре после начала атаки официальный аккаунт TJRS в Twitter предупредил сотрудников, чтобы они не входили в системы сети TJ локально или через удаленный доступ.

«В TJRS сообщает, что она сталкивается нестабильностью в компьютерных системах. Команда безопасности системы консультирует внутренние пользователь не для доступа к компьютерам удалена, ни войти в компьютеры в сети TJ,» чирикал в TJRS судебной системы.

Программа-вымогатель REvil, ответственная за кибератаку

Бразильский исследователь безопасности, известный как Brute Bee, поделился с BleepingComputer снимком экрана, на котором сотрудники делились записками о выкупе и обсуждали атаку друг с другом.

Эти записки о выкупе предназначены для операции вымогателя REvil, которая, как независимо подтвердил BleepingComputer, была ответственна за атаку.

BleepingComputer сообщили, что операция вымогателя REVil потребовала выкупа в размере 5 000 000 долларов за расшифровку файлов, а не за утечку данных.

В переведенной аудиозаписи, предоставленной BleepingComputer, человек описал атаку как «ужасную» и «худшее, что когда-либо там происходило», когда ИТ-персонал пережил «приступ истерического стресса», когда они спешили восстановить тысячи устройств.

Эта кибератака - не первая атака программ-вымогателей на судебные системы Бразилии.

В ноябре этого года на Верховный суд Бразилии напала банда вымогателей RansomEXX, которая начала шифрование устройств в середине судебных заседаний по видеоконференции.

В то же время веб-сайты других агентств федерального правительства Бразилии были отключены, но было неясно, были ли они закрыты в целях безопасности или подверглись атаке». ***(Lawrence Abrams. Brazil's Rio Grande do Sul court system hit by REvil ransomware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/brazils-rio-grande-do-sul-court-system-hit-by-revil-ransomware/). 29.04.2021).***

***

Програми-трояни

«Операторы нового троянца удаленного доступа (RAT) используют службу Telegram для сохранения контроля над своим вредоносным ПО.

Получивший название ToxicEye, RAT злоупотребляет Telegram как частью инфраструктуры управления и контроля (C2) для осуществления безудержной кражи данных.

В четверг Омер Хофман из Check Point Research сообщил в своем блоге, что новое удаленное вредоносное ПО было замечено в «дикой природе»: за последние три месяца было зарегистрировано более 130 атак.

Telegram - это канал связи и служба обмена мгновенными сообщениями, популярность которых в последнее время резко возросла из-за спорных изменений в политике обмена данными WhatsApp с Facebook.

Легитимная платформа, которая насчитывает более 500 миллионов активных пользователей в месяц, также оказалась популярной среди киберпреступников, использующих службу в качестве трамплина для распространения и развертывания вредоносных инструментов.

Цепочка атаки начинается с того, что операторы ToxicEye создают аккаунт Telegram и бота.

Боты используются для множества функций, включая напоминания, поиск, выдачу команд, а также для запуска опросов, среди других функций. Однако в этом случае бот встраивается в конфигурацию вредоносного ПО для злонамеренных целей.

«Любая жертва, зараженная этой вредоносной полезной нагрузкой, может быть атакована через бота Telegram, который подключает устройство пользователя обратно к C2 злоумышленника через Telegram», - говорят исследователи.

Фишинговые письма рассылаются предполагаемым жертвам, у которых есть вредоносные вложения в документы. Если жертва разрешает загрузку следующего вредоносного EXE-файла, ToxicEye развертывается.

ToxicEye RAT имеет ряд функций, которые можно ожидать от вредоносного ПО этой конкретной марки. Это включает в себя возможность сканирования и кражи учетных данных, данных операционной системы компьютера, истории браузера, содержимого буфера обмена и файлов cookie, а также возможность для операторов передавать и удалять файлы, прекращать процессы ПК и управлять задачами.

Кроме того, вредоносная программа может использовать кейлоггеры и взламывать микрофоны и периферийные устройства камеры для записи звука и видео. Исследователи также обнаружили особенности программ-вымогателей, в том числе способность шифровать и расшифровывать файлы жертв.

ToxicEye - последняя из разновидностей вредоносных программ, которые используют Telegram для поддержки C2, а уже готовые вредоносные программы с открытым исходным кодом, содержащие эту функцию, теперь стали обычным явлением.

Если вы подозреваете заражение, выполните поиск по запросу «C: \ Users \ ToxicEye \ rat.exe». Это подходит как для индивидуального, так и для корпоративного использования, и в случае обнаружения файл следует немедленно удалить из вашей системы.

«Учитывая, что Telegram можно использовать для распространения вредоносных файлов или в качестве канала C2 для удаленно контролируемых вредоносных программ, мы полностью ожидаем, что в будущем будут и дальше разрабатываться дополнительные инструменты, использующие эту платформу», - комментируют исследователи». ***(Charlie Osborne. ToxicEye: Trojan abuses Telegram platform to steal your data // ZDNet (https://www.zdnet.com/article/toxiceye-trojan-abuses-telegram-platform-to-steal-your-data/). 23.04.2021).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«В настоящей акции киберспецназа федералы удаленно удалили заражение, не предупредив предприятия заранее.

Федеральные органы удалили вредоносные веб-оболочки с сотен уязвимых компьютеров в Соединенных Штатах, которые были скомпрометированы с помощью печально известных уязвимостей ProxyLogon Microsoft Exchange.

ProxyLogon содержит группу ошибок безопасности, влияющих на локальные версии программного обеспечения Microsoft Exchange Server для электронной

почты. В прошлом месяце Microsoft предупредила, что ошибки активно используются постоянной устойчивой угрозой Hafnium (APT); после этого другие исследователи заявили, что 10 или более дополнительных APT также использовали их.

ProxyLogon состоит из четырех уязвимостей (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065), которые можно объединить в цепочку для создания эксплойта удаленного выполнения кода до аутентификации (RCE), что означает что злоумышленники могут захватить серверы, не зная каких-либо действительных учетных данных. Это дает им доступ к электронной почте и возможность установить веб-оболочку для дальнейшего использования в среде, например, для развертывания программ-вымогателей.

Хотя уровни установки исправлений увеличились, это не помогает уже скомпрометированным компьютерам.

«Многие владельцы зараженных систем успешно удалили веб-оболочки с тысяч компьютеров», - поясняет Министерство юстиции во вторник. «Другие, похоже, не смогли этого сделать, и сотни таких веб-оболочек сохранились без изменений».

Такое положение дел побудило ФБР принять меры; в иске, санкционированном судом, он отправил серию команд через веб-оболочки на затронутые серверы. Команды были разработаны для того, чтобы сервер удалял только веб-оболочки (идентифицируемые по их уникальному пути к файлу). Он не уведомил затронутые организации заранее, но власти заявили, что рассылают уведомления сейчас.

«Сегодняшнее санкционированное судом удаление вредоносных веб-оболочек демонстрирует стремление Департамента пресечь хакерскую деятельность с использованием всех наших юридических инструментов, а не только судебного преследования», - сказал в заявлении помощник генерального прокурора Джон Демерс из отдела национальной безопасности Министерства юстиции США.

Односторонние действия ФБР против эксплойтов ProxyLogon

Другие технические подробности акции держатся в секрете, но Эркан Чжэн, основатель и генеральный директор JupiterOne, отметил, что это беспрецедентное мероприятие.

«Что делает это действительно интересным, так это то, что суд распорядился удаленно исправить уязвимые системы», - сказал он по электронной почте. «Это произошло впервые, и, учитывая прецедент, вероятно, не последний. Многие предприятия сегодня не имеют представления о том, как выглядит их инфраструктура и состояние безопасности - прозрачность - огромная проблема для руководителей по информационной безопасности».

Дирк Шрейдер, вице-президент New Net Technologies по глобальным исследованиям в области безопасности, отметил, что отсутствие прозрачности ФБР может стать проблемой.

«В этом есть несколько критических моментов», - сказал он Threatpost. «Одно из них - ФБР, заявившее, что действие было вызвано тем, что у этих жертв отсутствует техническая возможность самостоятельно очистить свою

инфраструктуру, другое - похоже, что ФБР намерено отложить информирование жертв о самом удалении как минимум на месяц, ссылаясь на продолжающиеся расследования как на причину.»

Он пояснил: «Это может вызвать другие проблемы, поскольку у жертв нет возможности выяснить, к какой информации был получен доступ, установлены ли дополнительные бэкдоры и ряд других проблем, связанных с этим подходом».

Монти Кноде, директор по работе с клиентами и партнерами Horizon3.AI, отметил, что действие показывает, насколько опасны ошибки.

«Действия правительства всегда определяются властью, чтобы действовать», - сказал он по электронной почте. «Специально назвав «защищенные компьютеры» и объявив их «поврежденными», этого, по-видимому, было достаточно, чтобы дать ФБР подписанный ордер на выполнение такой операции без уведомления жертв перед проведением операции. Хотя масштабы операции неизвестны (отредактированы в постановлении суда), тот факт, что ФБР удалось выполнить менее чем за четыре дня, а затем публично объявить об этих усилиях, демонстрирует потенциальную угрозу национальной безопасности, создаваемую этими эксплуатируемыми системами и задействовано приоритетное планирование. Это не рефлексия».

По сообщению ФБР, эта операция была успешной при копировании и удалении веб-шеллов. Тем не менее, организациям все равно необходимо внести исправления, если они еще не сделали этого.

«В сочетании с усилиями частного сектора и других правительственных агентств на сегодняшний день, включая выпуск средств обнаружения и исправлений, мы вместе демонстрируем силу, которую государственно-частное партнерство привносит в кибербезопасность нашей страны», - сказал Денмерс. «Нет никаких сомнений в том, что еще предстоит проделать большую работу, но пусть также не будет сомнений в том, что Департамент привержен своей неотъемлемой и необходимой роли в таких усилиях».

Новые ошибки Exchange RCE и федеральное предупреждение

Эта новость последовала за апрельским патчем во вторник, в ходе которого Microsoft выявила больше уязвимостей RCE в Exchange (от CVE-2021-28480 до CVE-2021-28483), которые были обнаружены и сообщены Агентством национальной безопасности. Мандат федеральных агентств, чтобы исправить их в пятницу также вышел.

Кевин Брин из Immersive Labs, директор по исследованиям киберугроз, предупредил, что их использование в качестве оружия может произойти быстрее, чем обычно, поскольку мотивированные злоумышленники смогут использовать существующий концептуальный код.

«Это подчеркивает важность кибербезопасности сейчас для целых стран, а также продолжающееся стирание границ между национальными государствами, спецслужбами и безопасностью предприятий», - добавил он по электронной почте. «Учитывая, что в последнее время на широко используемое корпоративное программное обеспечение было совершено несколько громких атак, АНБ явно стремится активизировать свои действия и играть проактивную роль». ***(Tara Seals.***

FBI Clears ProxyLogon Web Shells from Hundreds of Orgs // Threatpost (https://threatpost.com/fbi-proxylogon-web-shells/165400/). 14.04.2021).

***

«Nintendo обратилась в суд с иском против Гэри Боузера, главы хакерской группировки Team Xecuter.

Компания Nintendo предъявила иск к руководителю хакерской группировки Team Xecuter Гэри Боузеру. Её лидеров задержали в Доминиканской Республике ещё в октябре 2020 года по подозрению в продаже инструментов для взлома и нелегального использования многих консолей. Хакерам грозит до 20 лет лишения свободы.

Судя по иску, Боузер и его напарник Макс Луарн занимались незаконной деятельностью по взлому и продаже инструментов для нелегального использования консолей Nintendo минимум с 2013 года.

Nintendo утверждает, что оборудование и программы, распространяемые Team Xecuter, якобы могут нанести вред 79 млн пользователей их консолей. Исходя из этого, компания требует от Team Xecuter по $2,5 тыс. за каждое устройство, которое они считают взломанным, и $150 тыс. за каждый факт нарушения интеллектуальной собственности Nintendo». ***(Nintendo подала в суд на хакера из Team Xecuter // SecurityLab.ru (https://www.securitylab.ru/news/519025.php). 18.04.2021).***

***

«Суд американского штата Вашингтон приговорил украинца Федора Гладыря к 10 годам лишения свободы за серию кибератак, которые привели к финансовым потерям в размере более $ 1 млрд. Об этом 16 апреля говорится в сообщении, опубликованном на официальном сайте Минюста США.

«Ответчик и его сообщники скомпрометировали миллионы финансовых учетных записей и причинили убытки американцам и экономике США в размере более чем на один миллиард долларов», — сообщает министерство юстиции США.

Граждан Украины Федора Гладыря, а также Дмитрия Федорова и Андрея Копакова задержали в 2018 году по обвинению в кибератаках против более чем 100 компаний. По данным Вашингтона, они состояли в хакерской группировке FIN7, атаковавшей компании в США, украли номера миллионов банковских карт, а также совершали взломы в Великобритании, Австралии и Франции». ***(Украинец получил 10 лет тюрьмы за кибератаки на американские компании // SecurityLab.ru (https://www.securitylab.ru/news/519015.php). 17.04.2021).***

***

«Один из участников группировки российских хакеров, которые похитили 15 млн рублей со счетов коммерческих организаций, задержан при попытке сбежать в Киргизию, сообщила официальный представитель МВД России Ирина Волк.

"На днях при попытке вылететь в город Бишкек Киргизской Республики задержан еще один фигурант. В настоящее время ему также предъявлено

обвинение в инкриминируемых деяниях и избрана мера пресечения в виде заключения под стражу. Предварительное расследование в отношении данного гражданина и остальных участников противоправной деятельности продолжается", - сказала она.

По данным следствия, с марта по декабрь 2018 года пятеро россиян из Орловской области, Кургана, Новосибирска и Санкт-Петербурга распространили в сети вирус, который помог им получить доступ к компьютерам ряда коммерческих организаций в РФ. Они смогли похитить 15 млн рублей, используя дистанционное управление программами банковского обслуживания. На данный момент правоохранительным органам удалось задержать четверых фигурантов». ***(Полиция задержала хакера, укравшего 15 млн. рублей // SecurityLab.ru (https://www.securitylab.ru/news/518973.php). 15.04.2021).***

***

«Миллионы адресов электронной почты, собранные ботнетом Emotet для кампаний по распространению вредоносных программ, были переданы Федеральному бюро расследований (ФБР) в рамках усилий агентства по очистке зараженных компьютеров.

Теперь частные лица и владельцы доменов могут узнать, повлиял ли Emotet на их учетные записи, выполнив поиск в базе данных по адресам электронной почты, украденным вредоносным ПО.

Собрано более 4 миллионов писем

Ранее в этом году правоохранительные органы взял под контроль инфраструктуру ботнета Emotet, в которую входили несколько сотен серверов по всему миру.

Используя линию связи с зараженными компьютерами, 25 апреля правоохранительные органы смогли разослать обновление, удаляющее вредоносное ПО Emotet во всех пораженных системах.

Помимо компьютерных систем, Emotet также взломал большое количество адресов электронной почты и использовал их для своих операций. ФБР теперь хочет дать владельцам этих адресов электронной почты быстрый способ проверить, не пострадали ли они от Emotet.

С этой целью агентство и Голландское национальное подразделение по тяжким техническим преступлениям (NHTCU) поделились 4 324 770 адресами электронной почты, которые были украдены Emotet, со службой уведомления о взломе данных Have I Been Pwned (HIBP).

Трой Хант, создатель службы HIBP, говорит, что 39% этих адресов электронной почты уже были проиндексированы как часть других инцидентов утечки данных.

Адреса электронной почты принадлежат пользователям из разных стран. Они поступали из логинов, хранящихся в инфраструктуре Emotet для рассылки вредоносных писем, или были получены из веб-браузеров пользователей.

Учитывая конфиденциальный характер данных Emotet, публичный поиск недоступен. По словам создателя HIBP Троя Ханта, подписчики сервиса, пострадавшие от взлома Emotet, уже были предупреждены.

Ссылаясь на процесс проверки, Хант говорит, что «людям нужно будет либо подтвердить контроль над адресом через службу уведомлений, либо выполнить поиск домена, чтобы увидеть, не затронуты ли они».

Национальная полиция Нидерландов, которая участвовала в операции по уничтожению Emotet, имеет аналогичную службу поиска, где пользователи могут проверить, не скомпрометировал ли Emotet их электронные письма.

Физические лица могут ввести адрес электронной почты, и если учетная запись является частью данных, изъятых из ботнета Emotet, голландская полиция отправит ей сообщение с инструкциями о том, что делать дальше. 3 февраля голландская полиция добавила к своей службе проверки 3,6 миллиона адресов электронной почты.

Другой сервис под названием Have I Been Emotet от компании по кибербезопасности TG Soft был запущен 1 октября 2020 года. Он проверяет, использовал ли Emotet адрес электронной почты в качестве отправителя или получателя. Однако последний раз он обновлялся 25 января, за два дня до отключения ботнета.

Огромные усилия по броскам

Emotet - один из самых известных ботнетов этого десятилетия, нанесший ущерб в сотни миллионов долларов по всему миру и заразивший около 1,6 миллиона компьютеров примерно за девять месяцев.

Он играл ключевую роль в цепочке распространения нескольких штаммов вымогателей, поскольку часто доставлял вредоносное ПО QakBot и Trickbot в скомпрометированную сеть, что в дальнейшем отбрасывало ProLock или Egregor, а также Ryuk и Conti соответственно.

27 января все три Эпохи - подгруппы ботнета с отдельной инфраструктурой - Emotet попали под контроль правоохранительных органов. Операция стала возможной благодаря усилиям властей Нидерландов, Германии, США, Великобритании, Франции, Литвы, Канады и Украины». ***(Ionut Ilascu. FBI shares 4 million email addresses used by Emotet with Have I Been Pwned // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fbi-shares-4-million-email-addresses-used-by-emotet-with-have-i-been-pwned/). 27.04.2021).***

***

Технічні аспекти кібербезпеки

«Крупная утечка маршрутизации BGP, произошедшая прошлой ночью, нарушила подключение к тысячам крупных сетей и веб-сайтов по всему миру.

Хотя утечка маршрутизации BGP произошла в автономной сети Vodafone (AS55410), расположенной в Индии, согласно источникам, она затронула американские компании, включая Google.

Утечка BGP вызывает 13-кратный всплеск неверно направленного трафика

Вчера компания Cisco BGPMon обнаружила несоответствие в системе интернет-маршрутизации, потенциально указывающее на некоторую деятельность

по перехвату BGP: «Префикс 24.152.117.0/24 обычно объявляется AS270497 RUTE MARIA DA CUNHA, BR».

«Но начиная с 15:07:01 2021-04-16, тот же префикс (24.152.117.0/24) также был объявлен ASN 55410», - говорится в сообщении BGPMon.

Дуг Мэдори, директор по анализу Интернета в Kentik, также подтвердил эти выводы, заявив, что автономная система ASN 55410 столкнулась с 13-кратным всплеском входящего трафика, направляемого к ней.

Это произошло из-за того, что сеть ошибочно объявила, что она поддерживает более 30 000 префиксов или маршрутов BGP, когда этого не произошло, в результате чего Интернет затопил эту сеть трафиком, который не должен был проходить через нее.

Указанная автономная система (AS55410) принадлежит Vodafone India Limited.

Согласно анализу Kentik, некоторые американские компании, в том числе Google, также пострадали в результате этого инцидента, который, по всей видимости, длился с 13:50 до 14:00 UTC 16 апреля 2021 года.

Кентик поделился с BleepingComputer еще некоторыми идеями:

«Этот инцидент повлиял на трафик всего на 10 минут, но за это время, вероятно, возникло бесчисленное множество проблем с подключением к Интернету для пользователей по всему миру».

«Любой, кто пытается получить доступ к веб-ресурсам, настроенным с использованием IP-адресов в маршрутах, которые были утекли, мог бы неправильно направить свой трафик на AS55410 в Индии, а затем отбросить его», - сказал BleepingComputer Дуг Мэдори из Kentik в интервью по электронной почте.

Хотя утечка в первую очередь повлияла на неправильное направление интернет-трафика для более 30 000 рекламируемых маршрутов и индийских пользователей Интернета, утечка действительно распространилась по всему миру, говорит Мадори.

Мадори сравнил неожиданный всплеск входящего трафика, испытанный Vodafone India (AS55410), по сути, с самовольной DDoS-атакой, которая также, вероятно, создала проблемы для пользователей Vodafone с выходом в Интернет в это время.

Дальнейший анализ, проведенный экспертом по BGP Анурагом Бхатиа, выявил более 20 000 префиксов из глобальных автономных сетей, которые пострадали в результате этого инцидента.

Что такое BGP, перехват BGP и утечка BGP?

BGP или протокол пограничного шлюза - вот что заставляет современный Интернет работать.

Это похоже на «почтовую систему» для Интернета, которая облегчает перенаправление трафика из одной (автономной) системы сетей в другую.

Интернет - это сеть сетей, и, например, пользователь, проживающий в одной стране, хотел получить доступ к веб-сайту, основанному в другой, должна быть система, которая знает, какие пути следует использовать при перенаправлении пользователя через несколько сетевых систем.

Это похоже на письмо, которое проходит через несколько почтовых отделений между его источником и местом назначения.

И это цель BGP: правильно направлять интернет-трафик по различным путям и системам между источником и местом назначения, чтобы Интернет функционировал.

Но BGP хрупок, и любые сбои или аномалии даже в нескольких промежуточных системах могут иметь длительное влияние на многие.

Чтобы Интернет работал, различные устройства (автономные системы) объявляют префиксы IP, которыми они управляют, и трафик, который они могут маршрутизировать. Тем не менее, это в значительной степени основанная на доверии система, предполагающая, что каждое устройство говорит правду.

Учитывая массивный взаимосвязанный характер Интернета, трудно добиться честности на каждом устройстве, присутствующем в сети.

Перехват маршрута BGP происходит, когда злоумышленник умудряется «ложно объявить» другим маршрутизаторам, что они владеют определенным набором IP-адресов, когда они этого не делают. Когда это происходит, возникает хаос.

Такая путаница в маршрутах создаст множество проблем в Интернете и приведет к задержкам, перегрузке трафика или полному отключению.

Но утечки маршрута BGP аналогичны перехвату маршрута BGP, за исключением того, что последнее более конкретно относится к случаям злонамеренной активности.

В то же время утечки на маршруте могут быть, скорее, случайными.

В любом случае утечки маршрута BGP или перехвата BGP автономная система (AS) объявляет, что она знает, «как» или «куда» направить трафик, предназначенный для определенных пунктов назначения (AS), о которых в действительности она не знает.

Это может привести к тому, что пользователь попадет по интернет-маршруту, который будет предлагать неоптимальную производительность или явным образом вызвать сбои и потенциально послужит прикрытием для действий по подслушиванию или анализу трафика в случаях злонамеренного угона.

Например, в прошлом году, как сообщает BleepingComputer, глобальный сбой IBM был вызван ошибочной конфигурацией маршрутизации BGP.

До этого мы видели значительный случай BGP угона в 2008 году, когда YouTube ушел в автономном режиме для глобальной аудитории из - за некоторые его трафик перенаправляет через пакистанские сервера.

В течение следующих нескольких лет мы сообщали о подобных инцидентах.

Как можно было предотвратить эту утечку BGP?

Хотя инцидент уже позади, он может повториться в любой момент.

Kentik поделился с BleepingComputer некоторыми общими мерами безопасности, которые компании могут использовать для защиты от утечек BGP, подобных этой, где говорится, что Kentik не был на месте вчера, когда произошла утечка.

«Очевидно, что в AS55410 не должно быть утечки 30 000 маршрутов, но в соседних сетях должны быть развернуты механизмы фильтрации для сдерживания

ущерба», - сказал Мадори BleepingComputer, объяснив, что эти механизмы включают в себя:

Установка MAXPREF: AS1273 (также зарегистрированный в Vodafone) и AS9498 (зарегистрированный в Bharti Airtel Ltd.) могли установить MAXPREF при их подключении к AS55410. Это простой механизм, который автоматически отключает соединение BGP, когда нисходящая сеть внезапно начинает отправлять неожиданно большое количество маршрутов BGP.

Настройка фильтров. Используя данные реестра маршрутизации в Интернете, AS1273 и AS9498 могли фильтровать маршруты, принятые от AS55410, зная, например, что они не должны получать маршруты BGP в США.

Развертывание RPKI: просочившиеся маршруты с авторизациями происхождения маршрута (ROA), настроенными в RPKI, должны были быть отброшены.

«В каждой утечке маршрутизации BGP участвует более одной стороны. Конечно, существует утечка, но всегда есть и другая сеть, которая распределяет просочившиеся маршруты в Интернет».

«Ошибки неизбежны, мы должны лучше заботиться друг о друге. В конце концов, Интернет - это коллективная работа!» - заключил Мадори в интервью BleepingComputer». ***(Ax Sharma. Major BGP leak disrupts thousands of networks globally // Bleeping Computer (https://www.bleepingcomputer.com/news/security/major-bgp-leak-disrupts-thousands-of-networks-globally/). 17.04.2021).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Согласно совместному отчету SAP и Onapsis, злоумышленники постоянно нацелены на новые уязвимости в приложениях SAP в течение нескольких дней после появления исправлений безопасности.

В некоторых случаях попытки эксплуатации наблюдались вскоре после обнародования ошибок безопасности: сканирование уязвимых систем началось через 48 часов после выпуска исправлений, а фактические попытки эксплуатации последовали примерно через 24 часа, анализ, который SAP и Onapsis проводили с середины 2020 года. выявил.

Приложения SAP, используемые в более чем 400 000 организаций (включая 1000 государственных и государственных организаций) для планирования ресурсов, управления жизненным циклом продукта, человеческим капиталом и цепочкой поставок, а также для различных других целей, представляют собой привлекательную цель для злоумышленников.

В ходе своего исследования обе организации наблюдали до 300 успешных попыток эксплуатации уязвимостей SAP. Атаки были нацелены на изменение

конфигураций и учетных записей пользователей, чтобы в конечном итоге получить доступ к бизнес-информации и украсть ее.

«Новые незащищенные приложения SAP, подготовленные в облачных средах (IaaS), были обнаружены и атакованы менее чем за три часа, что подчеркивает необходимость «сдвинуться влево» и обеспечить безопасное предоставление новых критически важных приложений с первого дня», - говорится в отчете.

Обе организации заявляют, что изощренные злоумышленники используют различные векторы атак для компрометации организаций через незащищенные приложения SAP, включая объединение нескольких уязвимостей, характерных для развертываний SAP.

Исследование также показывает, что злоумышленники предпринимают многочисленные попытки грубой силы нацеливаться на учетные записи пользователей SAP с высокими привилегиями, что еще раз показывает, что поддержание безопасных конфигураций системы так же важно, как и постоянное обновление программного обеспечения.

Эксплуатируемые уязвимости включают CVE-2020-6287 (также известную как RECON, эта критическая ошибка имеет оценку CVSS 10), CVE-2020-6207 (также оценка CVSS 10), CVE-2018-2380, CVE-2016-9563, CVE-2016-3976 и CVE-2010-5326. Успешное использование неисправленных ошибок SAP может привести к краже конфиденциальных данных, финансовому мошенничеству, нарушению критически важных бизнес-процессов и атакам программ-вымогателей и даже может вынудить организации полностью приостановить операции.

Однако, несмотря на известную нацеленность на уязвимые системы SAP, некоторые организации не могут своевременно применить доступные исправления. Таким образом, вместе с Агентством кибербезопасности и безопасности инфраструктуры (CISA) Министерства внутренней безопасности США (DHS) и Федеральным управлением кибербезопасности Германии (BSI) SAP и Onapsis рекомендуют организациям немедленно применять доступные исправления.

«Системы SAP с устаревшим или неправильно настроенным программным обеспечением подвергаются повышенному риску злонамеренных атак. Приложения SAP помогают организациям управлять критически важными бизнес-процессами, такими как планирование ресурсов предприятия, управление жизненным циклом продукта, управление взаимоотношениями с клиентами и управление цепочкой поставок», - отмечает CISA.

Организациям, использующим программное обеспечение SAP, рекомендуется выполнить оценку компрометации этих приложений, особенно для ресурсов с выходом в Интернет, оценить все приложения в среде SAP, выполнить оценку неправильной конфигурации и немедленно применить все доступные исправления, если это необходимо». ***(Ionut Arghire. Threat Actors Quick to Target (Patched) SAP Vulnerabilities // Wired Business Media (https://www.securityweek.com/threat-actors-quick-target-patched-sap-vulnerabilities). 06.04.2021).***

***

«Управление уязвимостями в значительной степени связано с управлением исправлениями: поиском, сортировкой и исправлением наиболее критических уязвимостей в вашей среде. Каждый аспект этого процесса представляет свои проблемы.

В 2020 году в NIST было сообщено о более чем 17000 уязвимостей, и более 4000 из них были высокоприоритетными. Знать, какие из них влияют на вас, где они находятся в вашем окружении и какие следует решать в первую очередь, является сложной задачей.

Randori, стартап, который разрабатывает автоматизированную платформу для атак красной команды, анонсировал Target Temptation, предназначенную для связывания активов и уязвимостей. Это показывает, где злоумышленники могут нанести удар, и выявляет уязвимости, которым следует уделить первоочередное внимание.

«Target Temptation предназначена для выявления «атакуемости» активов. Поверхность атаки компании может быть большой - часто тысячи целей. Компаниям сложно понять и расставить приоритеты, на чем им действительно нужно сосредоточиться, - говорит основатель и генеральный директор Randori Брайан Хаззард. «[Это] предназначено для того, чтобы раскрыть точку зрения атакующего на поверхность атаки, чтобы защитники могли понять, где атакующий, скорее всего, нанесет удар».

Дэвид (Мус) Вулпофф, соучредитель и технический директор Randori, поясняет в своем блоге: «Единственный способ сделать это - принять точку зрения злоумышленника. С этой точки зрения команды могут более эффективно управлять уязвимостями на поверхности атаки, не уделяя первоочередного внимания уязвимостям «высокой степени опасности», которые не представляют особой состязательности, и отдавая приоритет тем, которые могут быть использованы в качестве оружия. Хакеры ищут путь наименьшего сопротивления, что делает их достаточно предсказуемыми, если у вас есть достаточное количество информации о вашей поверхности атаки с их точки зрения».

Короче говоря, Target Temptation смотрит на уязвимости с точки зрения злоумышленников, а не просто на серьезность уязвимости. Многие уязвимости могут быть оценены как критические, но не обязательно представляют серьезную угрозу, потому что они не предлагают злоумышленнику путь к активам в конкретной среде. Target Temptation связывает серьезность возможного исхода с существованием уязвимостей, требующих принятия мер, чтобы выделить то, что следует обработать в первую очередь.

Вольпофф объясняет, как это работает. Первая часть - оценить потенциальную цель. «Модель состоит из двух основных частей, - сказал он: - это свойства самого программного обеспечения, а затем ситуация или контекст цели. Таким образом, первое, само программное обеспечение, будет включать уязвимости программного обеспечения или известные проблемы как единое целое, но также будет учитывать другие факторы, такие как функция программного обеспечения. Например, у сетей VPN есть критическая функция, они выходят за границы безопасности и вызывают повышенный интерес.

«Эти и другие факторы позволяют нам построить непрерывную оценку для программного обеспечения, то есть вероятность заинтересованности злоумышленника». Это позволяет Target Temptation понять потенциальные цели еще до того, как будет обнаружена соответствующая уязвимость, и поднять флаг перед защитниками.

Этот подход к управлению уязвимостями отличается от многих других тем, что он выделяет только соответствующие уязвимости, а не просто перечисляет все уязвимости. «Мы эмпирически знаем, - продолжил Вулпофф, - что подавляющее большинство уязвимостей в конечном итоге не используется. И это одна из проблем в области управления уязвимостями, из-за которой людям сложно расставить приоритеты».

Target Temptation устраняет те уязвимости, которые не имеют значения. Например, он может различать уязвимости, используемые конкретной библиотекой с открытым исходным кодом, и уязвимости в части библиотеки, которая не используется (см.: Зависимости библиотек и кошмар цепочки поставок с открытым исходным кодом). Он выделит те уязвимости, которые могут обеспечить путь к ценным активам, и проигнорирует остальные.

Вместо того, чтобы рассматривать уязвимости как проблему сами по себе, Target Temptation стремится выявить, что привлечет злоумышленников и почему. «Наши клиенты могут использовать наш продукт, чтобы наложить свои знания о том, что важно для бизнеса, - продолжил Вулпофф, - чтобы они могли предоставить данные о воздействии; и они объединяют эти две составляющие, чтобы сделать управление уязвимостями приоритетным. Если у высокоприоритетных активов есть набор проблем, мы можем указать механизмы их устранения. Там, где может не быть существующей проблемы, но есть актив, представляющий высокий риск, мы можем предоставить нашим клиентам более категоричные рекомендации о том, как обеспечить защитные стратегии для этих типов активов».

Target Temptation теперь доступна как часть платформы Randori Attack Platform и бесплатна для существующих клиентов.

«Сложность - друг нападающего и враг защитника», - резюмирует Хаззард. «На каждую 1000 обнаруженных активов часто приходится один, действительно интересный для злоумышленника. «Традиционные решения для управления поверхностью атаки (ASM) и управления уязвимостями выявляют тысячи проблем, усложняя и без того серьезную проблему. Директорам по информационной безопасности не нужно больше шума, им нужна ясность. С помощью Target Temptation Рандори дает защитникам представление о злоумышленнике, предоставляя доказательства, необходимые для четкого понимания их реального риска». ***(Kevin Townsend. Unearthing the 'Attackability' of Vulnerabilities that Attract Hackers // Wired Business Media (https://www.securityweek.com/unearthing-attackability-vulnerabilities-attract-hackers). 12.04.2021).***

***

«Критическая уязвимость, недавно исправленная поставщиком сетевых решений и решений для кибербезопасности Juniper Networks, может позволить

злоумышленнику удаленно захватить или нарушить работу затронутых устройств.

Брешь в безопасности, отслеживаемая как CVE-2021-0254 и влияющая на операционную систему Junos, была обнаружена Нгуеном Хоанг Тхучем, также известным как d4rkn3ss, исследователем из сингапурской компании STAR Labs, занимающейся кибербезопасностью.

Исследователь сообщил SecurityWeek, что об уязвимости, которая, по его словам, является самой серьезной ошибкой, которую он когда-либо обнаруживал в продукте Juniper, поставщику было сообщено более полугода назад.

В сообщении по безопасности, опубликованном на этой неделе, Juniper заявил, что уязвимость может быть использована удаленным злоумышленником, не прошедшим проверку подлинности, для выполнения произвольного кода или для запуска условия частичного отказа в обслуживании (DoS) на целевом устройстве. Эксплуатация уязвимости включает отправку специально созданных пакетов в целевую систему, и может быть запущена устойчивая DoS-атака путем непрерывной отправки вредоносных пакетов.

По словам Нгуена, злоумышленник, успешно воспользовавшийся этой уязвимостью, может получить root-доступ к целевой системе, а затем установить бэкдор или настроить устройство «любым способом». Уязвимость может быть использована сама по себе, и злоумышленнику не нужно связывать ее с другими уязвимостями.

Атаки из Интернета теоретически возможны, но уязвимые устройства обычно не доступны в Интернете. Исследователь считает, что если к такой системе можно получить доступ из Интернета, скорее всего, она неправильно настроена.

В своих рекомендациях Juniper пояснил: «Демон overlayd обрабатывает оверлейные пакеты OAM, такие как ping и traceroute, отправленные в оверлей. По умолчанию служба запускается от имени пользователя root и прослушивает UDP-соединения на порту 4789. Эта проблема возникает из-за неправильной проверки размера буфера, что может привести к переполнению буфера. Злоумышленники, не прошедшие проверку подлинности, могут отправлять специально созданные пакеты, чтобы активировать эту уязвимость, что может привести к удаленному выполнению кода».

Компания отметила, что демон оверлеев по умолчанию работает на маршрутизаторах серий MX и ACX и коммутаторах серии QFX. Другие платформы уязвимы, если настроена оверлейная сеть Virtual Extensible LAN (VXLAN).

Juniper заявила, что ей не известно о каких-либо злонамеренных атаках, использующих эту уязвимость, но отметила, что атака может быть запущена против конфигураций по умолчанию.

Агентство по кибербезопасности и безопасности инфраструктуры США (CISA) посоветовало организациям ознакомиться с рекомендациями Juniper и принять необходимые меры». ***(Eduard Kovacs. Critical Vulnerability Can Allow Attackers to Hijack or Disrupt Juniper Devices // Wired Business Media (https://www.securityweek.com/critical-vulnerability-can-allow-attackers-hijack-or-disrupt-juniper-devices). 16.04.2021).***

***

«Google Project Zero перейдет от довольно жесткого 90-дневного крайнего срока к новой модели, которая включает новый 30-дневный льготный период, чтобы дать пользователям время для установки исправлений до того, как будут раскрыты технические подробности.

В проекте сохраняется знаменитый 90-дневный период раскрытия уязвимостей, которые не были исправлены, однако, если исправление появится в течение периода раскрытия, технические подробности появятся через 30 дней после выпуска исправления.

Для эксплойтов в дикой природе раскрытие будет происходить через неделю после уведомления вместе с техническими деталями, если они не исправлены. Если патч выпущен в 7-дневном окне уведомлений, технические подробности появятся через 30 дней. Продавцы теперь могут запросить 3-дневный льготный период.

В редких случаях, когда Project Zero предоставил поставщикам двухнедельную отсрочку на раскрытие информации или новый трехдневный период для реальных эксплойтов, этот период будет использовать часть 30-дневной отсрочки для технических деталей.

В прошлом году Project Zero представил политику, по которой у поставщиков было полное 90-дневное окно, прежде чем оно раскрыло эксплойты.

Этот сдвиг также был сделан с целью ускорить установку пользовательских исправлений, но он был далек от успеха.

«Идея заключалась в том, что если поставщик хочет, чтобы у пользователей было больше времени для установки исправления, он будет отдавать приоритет доставке исправления раньше в 90-дневном цикле, а не позже», - написал менеджер Project Zero Тим Уиллис.

«На практике, однако, мы не наблюдали значительного сдвига в сроках разработки исправлений, и мы продолжали получать отзывы от поставщиков, что они обеспокоены публичным раскрытием технических подробностей об уязвимостях и эксплойтах до того, как большинство пользователей установят исправление. словами, предполагаемые сроки принятия исправления не были четко поняты».

Уиллис сказал, что в будущем начнется внедрение новой системы 90 + 30 дней, но политика должна начинаться с сроков, которые могут быть соблюдены поставщиками.

«Основываясь на текущем времени исправления уязвимостей для отслеживания данных, вполне вероятно, что мы сможем перейти к модели «84 + 28» на 2022 год (наличие крайних сроков, делимых на семь, значительно снижает вероятность того, что наши дедлайны выпадут на выходные)», - сказал он.

«Переход к модели «90 + 30» позволяет нам отделить время, необходимое для исправления, от времени принятия исправления, уменьшить количество споров вокруг компромиссов между атакующим и защитником и обмена техническими деталями, одновременно выступая за сокращение времени, которое заканчивается пользователи уязвимы для известных атак.

«Политика раскрытия информации - сложная тема, требующая множества компромиссов, и это решение было нелегким». ***(Chris Duckett. Google Project Zero***

testing 30-day grace period on bug details to boost user patching // ZDNet (https://www.zdnet.com/article/google-project-zero-testing-30-day-grace-period-on-bug-details-to-boost-user-patching/). 16.04.2021).

***

«Критическая уязвимость системы безопасности в устройстве VMware Carbon Black Cloud Workload может позволить повысить привилегии и получить административные права для решения.

Ошибка (CVE-2021-21982) занимает 9,1 балла из 10 по шкале серьезности уязвимости CVSS.

Платформа VMware Carbon Black Cloud Workload предназначена для обеспечения кибербезопасности виртуальных серверов и рабочих нагрузок, размещенных на платформе VMware vSphere. vSphere - это платформа виртуализации облачных вычислений VMware.

Согласно сообщению VMware, выпущенному на прошлой неделе, проблема в устройстве связана с неправильной обработкой URL-адресов.

«URL-адресом в административном интерфейсе устройства VMware Carbon Black Cloud Workload можно манипулировать для обхода аутентификации», - отметили в компании. «Злоумышленник, который уже получил сетевой доступ к административному интерфейсу устройства, может получить действительный токен аутентификации».

Это, в свою очередь, позволит злоумышленнику получить доступ к административному API устройства. После входа в систему как администратор злоумышленник может просматривать и изменять параметры административной конфигурации. В зависимости от того, какие инструменты организация развернула в среде, злоумышленник может провести ряд атак, включая выполнение кода, отключение мониторинга безопасности, перечисление виртуальных экземпляров в частном облаке и многое другое.

«Удаленный злоумышленник может использовать эту уязвимость, чтобы получить контроль над уязвимой системой», - говорится в сообщении Агентства по кибербезопасности и инфраструктуре (CISA) в одновременном предупреждении об ошибке.

Компаниям настоятельно рекомендуется обновить устройство VMware Carbon Black Cloud Workload до последней версии 1.0.2, которая содержит исправление.

Пользователи также должны ограничить доступ к локальному административному интерфейсу устройства только теми, кому он нужен, рекомендует VMware.

Обнаружил уязвимость Егор Димитренко из Positive Technologies...». ***(Tara Seals. Critical Cloud Bug in VMWare Carbon Black Allows Takeover // Threatpost (https://threatpost.com/critical-cloud-bug-vmware-carbon-black/165278/). 06.04.2021).***

***

«Группа исследователей безопасности, известная как Secret Club, отправилась в Twitter, чтобы сообщить об ошибке удаленного выполнения

кода в игровом движке Source 3D, разработанном Valve и используемом для создания игр с десятками миллионов уникальных игроков.

Уязвимость в игровом движке распространяется на продукты, созданные на его основе. В этом случае затронуты несколько игр, созданных с использованием Source, и для устранения риска для пользователей потребуется патч.

Один из исследователей в группе говорит, что они раскрыли уязвимость Valve около двух лет назад, но она продолжает влиять на последний выпуск Counter Strike: Global Offensive (CS: GO).

Некоторые из игр, которые используют движок Source от Valve, включают Counter-Strike, Half-Life, Half-Life 2, Garry's Mod, Team Fortress, Left 4 Dead и Portal.

Группу раздражает то, что по прошествии всего этого времени они не могут опубликовать технические подробности об ошибке, потому что ошибка все еще влияет на некоторые игры.

Награда выплачена, ошибка все еще активна

Флориан, студент, увлеченный реверс-инжинирингом, сообщил об ошибке удаленного выполнения кода (RCE) два года назад через программу вознаграждения за ошибки Valve на HackerOne.

Он сказал BleepingComputer, что уязвимость связана с повреждением памяти в исходном коде движка, поэтому она присутствует в нескольких играх. Исключение составляют игры, созданные с помощью Source 2, или игры, в которых используется модифицированная версия движка Source, например Titanfall.

Однако среди затронутых игр есть CS: GO, последнее обновление которого было 31 марта. В прошлом месяце в игре было около 27 миллионов уникальных игроков, согласно статистике на странице игры.

В разговоре с BleepingComputer Флориан сказал, что 10 апреля CS: GO все еще имеет уязвимый исходный код и что ошибка может быть использована для запуска произвольного кода на машине, на которой запущена игра.

Он сделал демонстрационное видео, показывающее, как злоумышленник может воспользоваться уязвимостью и выполнить код на целевом компьютере, просто отправив жертве приглашение в игру Steam.

Последний раз Флориан слышал от Valve около шести месяцев назад, когда Valve выплатила ему вознаграждение и заявила, что находится в процессе исправления проблемы и что она решила ее в одной конкретной игре с использованием движка Source.

Исследователь не раскрыл, какая игра получила исправление, но сообщил нам, что смог подтвердить действия Valve…

Флориан является членом Secret Club, некоммерческой группы реверс-инженеров, которые жаловались в Твиттере на то, что Valve так долго не решает проблему во всех играх.

Некоторые программы вознаграждения за ошибки на HackerOne имеют политику, которая позволяет исследователям раскрывать эксплойты или уязвимости, если исправление недоступно по истечении разумного периода, например 90 или 180 дней. Valve среди них нет.

Хотя Valve активно не мешает Флориану делиться подробностями, исследователь придерживается строгих этических принципов и знает, что полное раскрытие информации поставит под угрозу миллионы пользователей.

Исследователи утверждают, что Valve игнорирует отчеты

Карл Скоу, ведущий член Secret Club, сказал BleepingComputer, что злоумышленник может использовать эту уязвимость RCE для кражи конфиденциальной информации, такой как учетные данные или банковская информация.

Secret Club опубликовал несколько видеороликов, демонстрирующих эксплойты ошибок RCE в CS: GO от нескольких исследователей, утверждающих, что Valve игнорировала их в течение длительного периода, от пяти месяцев до года.

Ниже - от Бримко, Карла Смита и Саймона Сканнелла - показано использование уязвимости RCE движка Source при присоединении к вредоносному серверу сообщества.

Вот еще один, где RCE также достигается после подключения к вредоносному серверу. Инженер-программист Бьен Фам говорит, что они сообщили об этом Valve 2 апреля прошлого года, и компания проигнорировала их.

Неясно, все ли видео демонстрируют одну и ту же ошибку удаленного выполнения кода…». ***(Ionut Ilascu. CS:GO, Valve Source games vulnerable to hacking using Steam invites // Bleeping Computer (https://www.bleepingcomputer.com/news/security/cs-go-valve-source-games-vulnerable-to-hacking-using-steam-invites/). 12.04.2021).***

***

«Эксплуатация проблем позволяет злоумышленнику потенциально выполнить произвольный код на целевых системах.

В различных популярных программных приложениях был обнаружен ряд 1-Click уязвимостей, которые могут быть проэксплуатированы с помощью одного клика. Их эксплуатация позволяет злоумышленнику потенциально выполнить произвольный код на целевых системах.

Проблемы были обнаружены исследователями безопасности из компании Positive Security Фабианом Бройнлейном (Fabian Bräunlein) и Лукасом Эйлером (Lukas Euler) и затрагивают такие приложения, как Telegram, Nextcloud, VLC, LibreOffice, OpenOffice, кошельки Bitcoin/Dogecoin, Wireshark и Mumble.

«Настольные приложения, передающие задаваемые пользователем URL-адреса для открытия операционной системой, часто уязвимы к выполнению кода при взаимодействии с пользователем. Выполнение кода может быть достигнуто либо при открытии URL-адреса, указывающего на вредоносный исполняемый файл (.desktop,.jar,.exe и пр.) на доступном через интернет файловом ресурсе (nfs, webdav, smb и пр.), либо при появлении дополнительной уязвимости в URI-обработчике открытого приложения», — пояснили эксперты.

Уязвимости связаны с недостаточной проверкой введенного URL-адреса, который при открытии с помощью базовой операционной системы приводит к непреднамеренному запуску вредоносного файла.

Эксперты сообщили о своих находках разработчикам, и большинство приложений получили исправления:

Nextcloud — проблема (CVE-2021-22879) исправлена в версии 3.1.3;

Telegram — проблема была исправлена;

VLC Player — версия 3.0.13, исправляющая уязвимость, будет выпущена на следующей неделе;

OpenOffice — проблема будет исправлена в ближайшее время (CVE-2021-30245);

LibreOffice — исправлено в Windows, но ОС Xubuntu все еще уязвима (CVE-2021-25631);

Mumble — исправлена в версии 1.3.4 (CVE-2021-27229);

Dogecoin — исправлена в версии 1.14.3;

Bitcoin ABC — исправлена в версии 0.22.15;

Bitcoin Cash — исправлена в версии 23.0.0;

Wireshark — исправлена в версии 3.4.4 (CVE-2021-22191);

WinSCP — исправлена в версии 5.17.10 (CVE-2021-3331)». ***(В популярных настольных приложениях обнаружены 1-Click уязвимости // SecurityLab.ru (https://www.securitylab.ru/news/518985.php). 16.04.2021).***

***

«Эксплуатация проблем позволяет вызвать состояние «отказа в обслуживании» промышленных систем, утечку данных и удаленное выполнение кода.

Агентство кибербезопасности и безопасности инфраструктуры США (CISA) выпустило предупреждение о множественных уязвимостях в стеке OpENer EtherNet/IP. Эксплуатация проблем позволяет вызвать состояние «отказа в обслуживании» промышленных систем, утечку данных и удаленное выполнение кода.

Проблемы были обнаружены специалистами из компании Claroty и затрагивают все коммиты и версии OpENer, выпущенные до 10 февраля 2021 года. В общей сложности было обнаружено пять уязвимостей.

«Для эксплуатации уязвимостей злоумышленнику достаточно отправить на устройство специально созданные пакеты ENIP/CIP», — пояснили эксперты.

Первая уязвимость (CVE-2020-13556) записи за пределами поля в сервере Ethernet/IP может быть проэксплуатирована путем отправки серии специально созданных сетевых запросов для удаленного выполнения кода. Проблема получила оценку в 9,8 балла из максимальных 10 по шкале CVSS.

Другая уязвимость (CVE-2021-27478) связана с обработкой запросов Common Industrial Protocol (CIP) и позволяет осуществлять DoS-атаки. Еще одна (CVE-2021-27482) проблема представляет собой уязвимость чтения за пределами допустимого диапазона. С помощью специально созданных пакеты можно читать произвольные данные из памяти. Остальные две уязвимости (CVE-2021-27500 и CVE-2021-27498) также могут быть проэксплуатированы путем отправки специально созданных пакетов для проведения DoS-атак.

Поставщикам, использующим стек OpENer, рекомендуется выполнить обновление до последней версии, а также принять защитные меры, чтобы минимизировать уязвимость сети». ***(В стеке EtherNet/IP для промышленных систем обнаружены DoS-уязвимости // SecurityLab.ru (https://www.securitylab.ru/news/519006.php). 16.04.2021).***

***

«Российские специалисты нашли уязвимости в системе ЕАИСТО, которые помогают обходить новые правила техосмотра.

В Сети появилась информация о том, что заместитель начальника ГИБДД РФ Николай Шеюхин считает, что загружаемые фотографии транспортного средства при прохождении процедуры ТО могут быть подвержены изменению со стороны мошенников. Об этом сообщает «Коммерсантъ»

"Установленные требования к изображению транспортных средств не предусматривают защиту загружаемых фотоматериалов какими-либо техническими или программными средствами. Отсутствие защиты позволяет загружать модифицированные файлы с фотографическими изображениями, которые проходят форматно-логический контроль и полностью соответствуют требованиям приказа Минтранса № 97", - говорится в письме письмо Шеюхина Минтрансу РФ.

Согласно новым правилам, техосмотр обязательно сопровождается фотофиксацией автомобиля при заезде и выезде из сервиса. Эти фотографии будут заноситься в единую автоматизированную информационную систему техосмотра ЕАИСТО. На фото должны быть видны марка, цвет и регистрационный знак автомобиля, а также система будет включать координаты автомобиля и время прохождения осмотра.

Диагностические карты также можно оформить в электронном виде». ***(ГИБДД: Техосмотр уязвим перед хакерами // SecurityLab.ru (https://www.securitylab.ru/news/518757.php). 13.04.2021).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Последняя предварительная версия Microsoft для своего продукта повышенной безопасности Microsoft Defender for Endpoint теперь поддерживает неуправляемые устройства под управлением Windows, Linux, macOS, iOS и Android, а также сетевые устройства.

Общедоступная предварительная версия Microsoft Defender for Endpoint направлена на решение проблемы роста числа гибридных рабочих сред после пандемии, когда люди могут использовать свои собственные компьютеры и устройства из дома, а затем приносить их на работу и подключать к корпоративной сети.

«Самая опасная угроза - это та, о которой вы не знаете. Неуправляемые устройства - буквально одно из ваших самых слабых звеньев», - говорит Дэвид Уэстон, директор Microsoft по корпоративной безопасности и безопасности ОС.

«Умные злоумышленники идут туда первыми. При работе на дому угроза растет в геометрической прогрессии, что делает обнаружение и применение средств управления безопасностью к этим устройствам критически важным».

Microsoft Defender for Endpoint отличается от антивируса Microsoft Defender, который встроен во все устройства с Windows 10. Вместо этого он предлагает корпоративным группам безопасности средства реагирования на инциденты и инструменты расследования и работает как экземпляр в облаке Azure. Ранее он назывался Advanced Threat Protection в Microsoft Defender.

Новые возможности должны упростить обнаружение и защиту неуправляемых ПК, мобильных устройств, серверов и сетевых устройств в бизнес-сети.

Это предназначено для того, чтобы помочь ИТ-командам упростить настройку устройств для установки исправлений при наличии ошибок в операционной системе или программном обеспечении, а также решить проблемы приложений и устройств BYO, включая маршрутизаторы, брандмауэры и контроллеры WLAN.

«Как только сетевые устройства будут обнаружены, администраторы безопасности получат последние рекомендации по безопасности и уязвимостям на них», - сообщает Microsoft.

«Обнаруженные конечные точки (такие как рабочие станции, серверы и мобильные устройства) могут быть подключены к Microsoft Defender для конечных точек, что позволяет использовать все его возможности глубокой защиты».

Группы ИТ-безопасности могут протестировать общедоступную предварительную версию для неуправляемых устройств, включив функции предварительной версии для Microsoft Defender для конечных точек.

Продукт доступен со стандартным и базовым обнаружением, однако для общедоступной предварительной версии все клиенты будут иметь базовую версию. Он использует «одноадресные или широковещательные сетевые события, захваченные встроенными устройствами, для обнаружения неуправляемых конечных точек», - поясняет Microsoft в своем блоге.

«Базовое обнаружение использует двоичный файл SenseNDR.exe для пассивного сбора сетевых данных, и сетевой трафик не инициируется».

10 мая Microsoft планирует автоматически переключить всех клиентов с базового на рекомендованное им стандартное обнаружение, которое является активным методом обнаружения, который использует управляемые устройства для проверки сети на наличие неуправляемых устройств. Затем он использует интерфейсы обнаруженных устройств для сбора угроз, уязвимостей и метаданных, используемых для снятия отпечатков с устройств.

Microsoft заявляет, что она встроила средства управления конфиденциальностью, чтобы предотвратить обнаружение этой функцией частных устройств, используемых дома, таких как интеллектуальные устройства, телевизоры и игровые консоли.

"Существует встроенная логика, чтобы предотвратить это, и уровень контроля, чтобы определить, с какими сетями работает этот процесс обнаружения. Логика была разработана, чтобы различать корпоративные сети и некорпоративные сети, чтобы избежать обнаружения частных или общедоступных устройств, не - контролируется организацией. Существуют строгие условия, гарантирующие, что такие устройства не будут обнаружены и представлены на портале», - поясняет Microsoft». ***(Liam Tung. Microsoft Defender for Endpoint now protects unmanaged BYO devices // ZDNet (https://www.zdnet.com/article/microsoft-defender-for-endpoint-now-protects-unmanaged-byo-devices/). 14.04.2021).***

***

«Infinidat объявляет об улучшении возможностей восстановления данных в InfiniGuard для корпоративных пользователей. Новая функциональность InfiniGuard CyberRecovery обеспечивает лучшую в своем классе защиту всей среды резервного копирования. Она включает в себя создание неизменяемых моментальных снимков и почти мгновенное восстановление предыдущих состояний системы на основе определенных заказчиком политик. Эти уникальные нововведения направлены на устранение угроз кибератак программ-вымогателей, которые происходят в среднем каждые 14 секунд.

«Почти мгновенное восстановление данных с решением InfiniGuard после кибератак дает возможность Infinidat значительно повысить планку защиты от вымогателей, — говорит Фил Буллинджер (Phil Bullinger), генеральный директор Infinidat. — Заметные усовершенствования нашей платформы InfiniGuard значительно улучшают процесс защиты данных. Мы даем возможность корпоративным клиентам создать новую линию защиты для резервного копирования данных, что будет играть значительную роль как в 2021 году, так и в будущем».

InfiniGuard CyberRecovery борется с растущим количеством угроз программ-вымогателей и вредоносных вторжений в центры обработки данных крупных компаний, а также поставщиков облачных услуг. Захватив данные, вымогатели уничтожают резервные копии, крадут учетные данные и передают украденную информацию. Это приводит к тому, что предприятиям абсолютно любых размеров приходится прекращать деятельность в одночасье. И нет ничего необычного в том, что компании платят большие суммы денег для восстановления бизнеса.

«Поскольку атаки вымогателей уже обходятся крупным организациям в 20 миллиардов долларов в год, ИТ-директора должны выйти за рамки простого резервного копирования, чтобы внедрить всеобъемлющую и высоконадежную стратегию кибербезопасности, — добавляет Эрик Бургенер (Eric Burgener), вице-президент по исследованиям группы инфраструктурных систем, платформ и технологий IDC. — Эта стратегия должна обеспечить прозрачность процессов резервного копирования на основе определенных политик и с использованием неизменяемых моментальных снимков, а также гибкое, гранулярное и высокопроизводительное восстановление данных. И все это подразумевает необходимость внедрения архитектуры защиты данных следующего поколения».

Обнаружение того, как именно вымогатели проникают в ИТ-инфраструктуру, является чрезвычайно сложной задачей и часто происходит после того, как ущерб уже нанесен. Возможности для атак значительно выросли за последний год из-за увеличения количества сотрудников, работающих из дома. Традиционной линией обороны было резервное копирование данных, но кибертеррористы теперь атакуют резервные копии и системы хранения, в которых они находятся. Именно поэтому резервное копирование данных само по себе уже не является достаточной защитой.

InfiniGuard CyberRecovery защищает само решение резервного копирования с помощью прозрачного и понятного функционала, который представляет собой подход нового поколения к защите от программ-вымогателей и других киберугроз. InfiniGuard создает неизменяемые моментальные снимки с использованием технологии WORM (write once read many), гарантирующей, что копии данных не могут быть удалены, зашифрованы или изменены.

Обновленное решение Infinidat для кибервосстановления также использует возможности восстановления данных к их предыдущим состояниям в соответствии с заданными политиками. Это позволяет достичь почти мгновенного восстановления к любой точке в истории данных для обеспечения их целостности и согласованности. Для компаний, которые хотят проверить данные до того, как они вернутся в оперативную среду бизнеса, InfiniGuard предоставляет изолированную тестовую среду, которая очень проста в использовании.

«Защита всей среды резервного копирования теперь является неотъемлемой частью стратегии киберзащиты любой организации, — отмечает Грег Харрисон (Greg Harrison), вице-президент по глобальным проектам в CBTS. — InfiniGuard CyberRecovery предлагает нашим клиентам новый мощный способ защиты от растущих угроз. Быстрая скорость, с которой вы можете восстановить данные, сохранив их целостность, делает InfiniGuard звездой кибервосстановления».

Инновации Infinidat в области кибервосстановления на платформе InfiniGuard дают корпоративным клиентам возможность реализовать новую, более эффективную стратегию защиты от кибератак, борьбы с ними и восстановления после них». ***(Владимир Бахур. Infinidat помогает компаниям бороться с атаками программ-вымогателей // CNews (https://www.cnews.ru/news/line/2021-04-07_infinidat_pomogaet_kompaniyam). 07.04.2021).***

***

«Лаборатория Касперского» представила промышленный шлюз данных Kaspersky IoT Secure Gateway 100 на базе KasperskyOS. Он позволяет подключать полевые устройства и сенсоры к сервисам промышленного интернета вещей (IIoT), обеспечивая защиту данных, собираемых с оборудования, и их безопасный перенос в цифровые приложения.

Согласно исследованию Juniper Research, ожидается, что к 2025 г. количество IIoT-соединений во всём мире вырастет на 107% и достигнет 36,8 млрд. Сбор и обработка данных с IIoT-датчиков на оборудовании помогает предприятиям лучше понимать рабочие процессы, делает возможным диагностическое обслуживание, повышает эффективность и производительность. Однако основная проблема заключается в том, как связывать промышленную сеть с корпоративной цифровой

экосистемой так, чтобы собирать как можно больше информации с оборудования, преобразовывать её и безопасно отправлять на специальную платформу для хранения и обработки.

Kaspersky IoT Secure Gateway 100 обеспечивает прямое защищённое подключение к промышленным доменам с прессовым оборудованием, конвейерами, станками ЧПУ и другими устройствами. Этот продукт был разработан на базе аппаратной платформы Siemens SIMATIC IOT2040 и операционной системы KasperskyOS. Он соответствует концепции кибериммунности, созданной «Лабораторией Касперского». Благодаря Kaspersky Security System, микроядру KasperskyOS и архитектуре множественных независимых уровней безопасности (MILS) шлюз может выполнять только те действия, которые были предусмотрены на этапе проектирования. Это означает, что большинство традиционных кибератак на кибериммунный шлюз не могут быть эффективными и влиять на его основные функции. Поэтому нет необходимости в дополнительной защите шлюза и подключённого оборудования, такой как антивирус, контроль устройств, диод данных и другие.

Шлюз подходит для развёртывания в инфраструктуре с разнообразным оборудованием различных производителей благодаря использованию универсального коммуникационного протокола OPC UA. Kaspersky IoT Secure Gateway 100 имеет встроенное соединение с Siemens MindSphere — облачной сервисной цифровой IIoT-платформой. Все функциональные компоненты шлюза были разработаны дочерней компанией «Лаборатории Касперского» — НПО «Адаптивные промышленные технологии» («Апротех»), которая является официальным партнёром Siemens. Совместное решение обеспечивает быстрый доступ к промышленным данным, которые преобразуются в бизнес-результаты с помощью индустриальных приложений с передовой аналитикой и искусственным интеллектом.

«Цифровые технологии быстро меняются, и в последнее время мы видим, что кибербезопасность оказалась одной из наиболее актуальных глобальных проблем. Наша концепция кибериммунности позволяет создавать различные ИТ-решения с «врожденной» защитой на базе операционной системы KasperskyOS. Такие решения способны противостоять подавляющему большинству видов кибератак», — сказал Григорий Сизов, руководитель направления по развитию бизнеса KasperskyOS.

«Цифровая трансформация создаст новые ведущие компании с внедрёнными IIoT-экосистемами. Передовые технологии, новые навыки и инновационные бизнес-модели необходимы для перемен наряду с новым уровнем устойчивости. Сегодня мы с гордостью анонсируем Kaspersky IoT Secure Gateway 100 как неотъемлемую часть выигрышной комбинации и первое решение из числа кибериммунных», — отметил Андрей Суворов, генеральный директор компании «Апротех». ***(«Лаборатория Касперского» представила промышленный шлюз данных Kaspersky IoT Secure Gateway 100 на базе KasperskyOS // CNews (https://safe.cnews.ru/news/line/2021-04-15_laboratoriya_kasperskogo). 15.04.2021).***

***

«Технология блокчейн помогает миру в большем количестве способов, чем мы можем себе представить, и один из них - это область кибербезопасности, которая включает в себя некоторые из самых важных отраслей в мире, таких как финансы и здравоохранение. С ростом числа киберпреступлений, включая кражи в Интернете и даже доксинг, миру требуется немедленное решение, и блокчейн может предоставить его, потому что он выходит далеко за рамки обычных советов по покупке биткойнов и альткойнов. Мир киберпреступности развивается так же быстро, как и развитие технологий, но благодаря блокчейну мы можем иметь преимущество над преступниками. Давайте рассмотрим 5 случаев, которые доказывают, что блокчейн - это то, что нам нужно для более безопасного кибер-мира, потому что в нескольких отраслях уже требуются быстрые и безопасные решения. Безопасность для Интернета вещей (IoT) Интернет вещей растет впечатляющими темпами: согласно прогнозам Mordor Intelligence, к 2027 году его стоимость превысит 1000 миллиардов долларов. Однако пространство IoT находится под угрозой кибератак и хакеров. К счастью, технология блокчейн предлагает простое решение для решения этих проблем. Проще говоря, это позволяет различным устройствам обмениваться данными без помех и нарушений. На самом деле есть много проектов, которые уже работают над решением этих вопросов. Вот самые популярные:

VeChain IOTA DigiByte IOST Helium

Поскольку Интернет вещей - это горячая отрасль, которая быстро растет, было бы неплохо инвестировать в эти токены, поскольку в ближайшие годы цены на их криптовалюту могут вырасти. Один только VeChain сильно вырос за последние несколько недель, и, согласно последним прогнозам, он может продолжить устойчивый рост во время этого бычьего рынка. Это один из наиболее быстро развивающихся секторов, и, следовательно, блокчейн действительно показывает свой потенциал, поскольку он уже применяется в реальных проектах, которые представляют его в положительном свете. Надежная безопасность DNS Система доменных имен отвечает за работу Интернета во многих смыслах. Однако он страдает теми же проблемами, что и аналогичные типы технологий: они уязвимы для взломов, атак и утечки данных. Еще раз, технология блокчейн может решить эту проблему. Шифрование данных и использование сложных протоколов позволяют скрыть важную информацию, такую как IP, имена, адреса и т. Д. Внедряя эти достижения в технологии блокчейн, мы можем наслаждаться большей безопасностью, особенно если мы участвуем в различных проектах цифрового маркетинга, где наша конфиденциальность абсолютно необходима. Это решит такие проблемы, как доксинг, потому что может сделать кого-то действительно анонимным в Интернете. В следующем разделе мы поговорим о шифровании данных и о том, как технология блокчейн подняла его на новый уровень. Шифрование данных Технология блокчейн широко известна своими достижениями в области шифрования данных, которые делают возможным существование. Однако не все криптовалюты используют шифрование, самым популярным примером является сам биткойн. Однако у нас есть много монет, которые действительно реализуют продвинутые протоколы шифрования.

Вот самые важные из них: Monero DASH Zcash Horizen

Таким образом, эти достижения в технологии шифрования могут помочь нам повысить уровень наших ресурсов кибербезопасности, поскольку они могут защитить коммуникации и важную информацию, помогая таким отраслям, как банковское дело, финансы, логистика, здравоохранение и т. д.

Противодействие DDoS-атакам Блокчейн также может помочь против DDoS-атак и других угроз вредоносного ПО, поскольку его безопасная и неподкупная структура может защитить от них онлайн-ресурсы. В последнее время количество DDoS-атак растет, особенно с учетом того, что экономика день ото дня становится цифровой, чему способствует текущий контекст COVID-19. Усложняя совершение этих атак и решая их быстро и эффективно, мы можем повысить безопасность и стабильность веб-сайтов и владельцев онлайн-собственности, поскольку DDoS-атака может нанести большой ущерб с точки зрения потери денег и репутации. Децентрализованное хранилище данных Блокчейн - это децентрализация данных, и, следовательно, это еще одно отличное применение, которое может улучшить кибербезопасность. Это особенно важно для правительств, корпораций и международных компаний, которым необходимо безопасно и эффективно хранить и обрабатывать огромные объемы данных. Используя решения на основе блокчейнов, компании могут защитить свои ценные данные от взлома, а также за считанные секунды передать их на любой сервер, который они используют. Это особенно важно, если вам нужно управлять конфиденциальной информацией, например, финансовой. Используя решения блокчейн, вы можете избежать множества потенциальных проблем. Заключительные слова Как видите, технология блокчейн уже улучшает мир кибербезопасности, и дела будут только улучшаться. Блокчейн развивается быстрыми темпами, и, поскольку он реализуется в реальных проектах, мы можем только ожидать увидеть еще больше результатов в ближайшем будущем». ***(MIC JOHNSON. 5 Cases of Blockchain for Cybersecurity // latesthackingnews.com (https://latesthackingnews.com/2021/04/27/5-cases-of-blockchain-for-cybersecurity/). 27.04.2021).***

***

«Ни дня не проходит без заголовков о кибератаках и утечках данных. Чтобы не отставать от кибератак, организациям необходимо быть на шаг впереди плохих парней. Недостаточно иметь лучшие инструменты кибербезопасности. Организациям также необходимо работать вместе, сотрудничать и обмениваться друг с другом информацией об угрозах и безопасности. Представляем StrikeReady, стартап в области кибербезопасности из Пало-Альто, Калифорния, который объединяет организации для создания устойчивой среды кибербезопасности.

После десятилетий опыта в области кибербезопасности и общения с сотнями аналитиков по кибербезопасности и директоров по информационной безопасности команда StrikeReady определила три ключевые проблемы для модернизации операций по обеспечению безопасности: нехватка навыков кибербезопасности, нехватка специалистов по кибербезопасности и проблема сотрудничества.

Для решения этих проблем StrikeReady построила облачную платформу для операций и управления безопасностью, которая максимизирует отдачу от

существующих инвестиций организации в безопасность - людей, процессов и продуктов. Платформа интегрирует, вводит в действие, оптимизирует и консолидирует разрозненные продукты безопасности, а также помогает командам по кибербезопасности и расширяет их возможности. Конвергенция ИИ, данных и автоматизации помогает защитникам быстро реагировать на инциденты, активно защищаться от возникающих угроз и / или действовать молниеносно.

Сегодня StrikeReady появляется незаметно с начальным финансированием в размере 3,6 млн долларов для ускорения вывода на рынок и продаж, а также для развития команды НИОКР. Посевной раунд проводился 11.2 Capital при участии Outlier Venture Capital и нескольких бизнес-ангелов из Кремниевой долины.

Команда StrikeReady, основанная в 2019 году, возглавляется Ясиром Халидом, бывшим инженером и архитектором основных технологий обнаружения в FireEye, где он провел десять лет и его работа привела к получению более пятнадцати патентов в области кибербезопасности при поддержке CPO, Anurag Gurtu, ранее возглавлял отдел маркетинга продуктов безопасности (UEBA) в Splunk, а до этого возглавлял технический маркетинг FireEye и управление продуктами в Cisco.

Большинство сотрудников StrikeReady - это новички из FireEye, имеющие большой опыт работы с различными стеками безопасности - сетевой безопасностью, безопасностью конечных точек, безопасностью электронной почты, облачной безопасностью и автоматизацией. Эта бывшая команда FireEye сыграла важную роль в исследовании угроз, анализе угроз, исследованиях и разработках, проектировании и продажах. Менее чем за два года команда успешно развернула продукт на нескольких средних и крупных предприятиях и государственных учреждениях в США и за рубежом.

Ясир Халид, основатель и генеральный директор StrikeReady, сказал: «Наше видение состоит в том, чтобы использовать ориентированный на человека подход, чтобы сделать команду безопасности эффективной и исключительно эффективной, при этом превратив всех аналитиков в области кибербезопасности в экспертов и без обучения без отрыва от работы. ”

Комментируя инвестиции, Прамод Госави, директор 11.2 Capital, сказал: «Предположим, что вас взломают - это новая норма для индустрии кибербезопасности, поскольку злоумышленники масштабируют свои атаки с помощью автоматизации, а организациям необходимо применять аналогичные методы. подход. Конвергенция ИИ, знаний и автоматизации является обязательным условием повышения производительности аналитиков безопасности и сокращения их нехватки навыков. Основатели StrikeReady, Ясир и Анураг, обладают глубокими знаниями в области операций по обеспечению безопасности и автоматизации на базе искусственного интеллекта. Они создали уникальный продукт, который ускоряет расследование инцидентов, автоматизирует реагирование, передает знания и проактивно защищает организацию. 11.2 Capital рада поддержать миссию команды по обеспечению безопасности в будущем». ***(Nickie Louise. Cybersecurity startup StrikeReady emerges from stealth with $3.6M in seed funding to create a resilient cybersecurity environment // TechStartups.com***

(https://techstartups.com/2021/04/28/cybersecurity-startup-strikeready-emerges-stealth-3-6m-seed-funding-create-resilient-cybersecurity-environment/). 28.04.2021).

***