**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

№ 9 (вересень)

Київ – 2022

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2022.– №9 (вересень) . – 311 с.

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

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

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

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

ЗМІСТ

Стан кібербезпеки в Україні 4
Кібервійна проти України 4
Боротьба з кіберзлочинністю в Україні 19
Міжнародне співробітництво у галузі кібербезпеки 22
Коронавірус COVID-19 та питання кібербезпеки 23
Світові тенденції в галузі кібербезпеки 24
Сполучені Штати Америки та Канада 71
Країни ЄС та Великобританія 103
Російська Федерація 123
Австралія 124
Інші країни 126
Кібервійни та протидія зовнішній кібернетичній агресії 132
Створення та функціонування кібервійськ 152
Кіберзахист критичної інфраструктури 153
Захист персональних даних 159
Кібербезпека Інтернету речей 179
Кіберзлочинність та кібертероризм 185
Діяльність хакерів та хакерські угруповання 234
Вірусне та інше шкідливе програмне забезпечення 238
Фішингові атаки 275
Технічні аспекти кібербезпеки 286
Виявлені вразливості технічних засобів та програмного забезпечення 296
Технічні та програмні рішення для протидії кібернетичним загрозам 302

«Фонд соціального страхування України (ФССУ) проводить закупівлю обладнання для модернізації дата-центру з ліцензійним програмним забезпеченням.

Про це ФССУ повідомляє в Телеграмі, передає Укрінформ.

«На виконання доручення Прем'єр-міністра України Дениса Шмигаля з метою забезпечення кіберзахисту критичної інформаційної інфраструктури Фонд соціального страхування України проводить закупівлю обладнання для модернізації дата-центру з ліцензійним програмним забезпеченням», - йдеться в повідомленні.

Зазначається, що обладнання буде інтегроване з Єдиною інформаційно-аналітичною системою Фонду та забезпечить збереження і надійний захист бази даних, зокрема, персональних даних мільйонів застрахованих осіб, їх роботодавців, потерпілих на виробництві та їх родин в умовах потенційної кібернебезпеки з боку країни-агресора.

Також модернізація серверів дозволить забезпечити безперебійне функціонування єдиної системи Фонду, опрацювання заяв-розрахунків і проведення виплат лікарняних, декретних, допомог на поховання і страхових виплат.

У Фонді наголошують, що закупівля є плановою та проводиться відповідно до визначених видатків за цим напрямом у бюджеті ФССУ на 2022 рік… ***(Фонд соцстраху модернізує дата-центр для посилення кіберзахисту // Укрінформ (https://www.ukrinform.ua/rubric-technology/3568217-fond-socstrahu-modernizue-datacentr-dla-posilenna-kiberzahistu.html). 10.09.2022).***

***

Кібервійна проти України

«З 29 серпня до 11 вересня українська ІТ-армія паралізувала понад 2400 російських онлайн-ресурсів, зокрема російські медіа та сайти найбільших банків рф.

…про це повідомляє пресслужба Міністерства цифрової трансформації у Фейсбуці.

«Цифрова бавовна від ІТ-армії: понад 2400 паралізованих онлайн-ресурсів за 2 тижні. ЗСУ продовжують звільняти Україну від окупантів, а ІТ-армія – розхитувати економіку ворога та деморалізувати росіян на цифровому фронті», - йдеться в повідомленні.

Зазначається, що українським фахівцям вдалось паралізувати сервіси Газпромбанку, Московського КредитБанку та Совкомбанку. Через це росіяни не змогли скористатися онлайн-банкінгом та провести фінансові операції зі смартфону, а також отримати зарплати, а їхні рідні – компенсації.

Кіберспеціалісти призупинили роботу найбільшого онлайн- майданчика з продажу автомобілів та запчастин – Дром, що унеможливило росіянами купівлю

автомобілів або запчастини для солдат. Кібератака вивела з ладу й великі пропагандистські російські медіа – Rambler, Газета.Ru, МК.

Також під український «плив» потрапили системи електронного документообігу у підприємств з молочної продукції. Оптові та роздрібні продавці молочної продукції вимушені відтепер вручну обробляти документи.

У міністерстві додали, що айтівці попіклувалися і про те, щоб на центральних телеканалах Криму школярі та студенти отримали привітання з 1 вересня від Президента України…» ***(Українська ІТ-армія за два тижні паралізувала роботу низки російських медіа та банків // Укрінформ (https://www.ukrinform.ua/rubric-technology/3569643-ukrainska-itarmia-za-dva-tizni-paralizuvala-robotu-nizki-rosijskih-media-ta-bankiv.html). 12.09.2022).***

***

«Росія почала здійснювати масштабні кібератаки на Україну за пів року до повномасштабного військового вторгнення 24 лютого.

…про це заявив віцепрем'єр-міністр - міністр цифрової трансформації України Михайло Федоров під час щорічної конференції «Ялтинська європейська стратегія».

«Кібервійна розпочалась задовго до повномасштабного вторгнення. Вона почалась по факту десь за пів року», - сказав він.

За словами Федорова, за пів року до 24 лютого розпочались масштабні кібератаки хакерських угруповань фсб росії. Це були багатовекторні атаки, метою яких було нанести максимальну шкоду українській інфраструктурі і виявити, як працюють інформаційні системи в Україні та як вони захищені.

«По факту десь ще у жовтні-листопаді почались найпотужніші атаки, з якими ми вчились працювати та від яких ми будували систему захисту», - розповів віце-прем'єр.

Федоров зазначив, що Україні вдалось захиститись від цих та подальших кібератак завдяки створенню спеціальної команди при Держспецзв'язку, яка відпрацьовувала різні сценарії атак та захисту від них…». ***(Хакери фсб атакували Україну за пів року до повномасштабної війни – Федоров // Укрінформ (https://www.ukrinform.ua/rubric-technology/3568970-hakeri-fsb-atakuvali-ukrainu-za-piv-roku-do-povnomasstabnoi-vijni-fedorov.html). 11.09.2022).***

***

«…За даними компанії з кібербезпеки Mandiant, Росія розпочала кібератаки проти України за кілька тижнів до того, як перші танки перетнули кордон. За оцінками експертів, це були стримані операції хакерів, пов'язаних із СЗР, ФСБ та ГРУ РФ.

Спочатку запустили шкідливе програмне забезпечення Wiper, яке стирає жорсткі диски заражених ним пристроїв. Атаку націлили на кілька державних, некомерційних організацій та організацій, які займаються інформаційними технологіями в Україні. Потім запустили ПЗ Gamaredon, пізніше атакували понад 10 тис. супутникових інтернет-модемів Viasat в Україні та інших частинах Європи. За кілька днів об'єктом кібератаки стала українська атомна енергетична компанія, а також медіакомпанії та державні установи, про що повідомляла Microsoft. 12 квітня

здійснили невдалу спробу атакувати енергосистему за допомогою ПЗ Sandworm з метою відключити електроенергію.

Крім цих інцидентів, атаки зазнали фінустанови, пункти прикордонного контролю, інтернет-інфраструктура, що призвело до збоїв у роботі банківських послуг, відключення електроенергії, порушення логістичних ланцюжків. Здійснювали фішингові атаки на уряд і військових, а також запуск софту, який крав інформацію. Постійно здійснювали DDoS-атаки проти телеком-компаній.

Російські кібероперації виявилися неефективними та проводилися на рівні розіграшів. А розіграші ніколи не допомагали вигравати війни, йдеться у статті.

Що стало очевидним за останні 6 місяців, так це те, що мало що з російських кібератак здійснили на підтримку чіткої військової мети. Не було жодних нападів на системи військового управління, жодних атак на критичну інфраструктуру і нічого, що могло б чинити реальний тиск на Україну, щоб змусити її чи її союзників піти на поступки. Натомість російська кіберкампанія була стриманою та незалежною від реального військового вторгнення. Чому?

Перша причина полягає в тому, що Росія не спромоглася координувати свої військові операції. Наприклад, у НАТО сухопутні, морські, повітряні та космічні сили діють як єдина бойова одиниця, а у ЗС РФ навіть наземні сили не могли нормально скоординуватися.

Друга причина. Звичайна війна і кібервійна дуже різняться. Звичайна війна спрямована на знищення людей та об'єктів, захоплення територій. У кібервійні ціллю є інформація. Територія тут не має значення. Ціль полягає в тому, щоб захопити якомога більше важливих даних і позбавити доступу до них. В результаті ці два типи війни часто мають цілі, що суперечать одна одній, тому, можливо, Росія вирішила поки не діяти занадто завзято в кіберпросторі, а зосередитися на розвідувальних завданнях, пише ЗМІ.

Третім фактором є кіберзахист України: 2022 — не перший рік, коли Росія нападає на країну. Україна стала цифровим полігоном для Росії після революції 2014 року, внаслідок якої повалили промосковський уряд. Це перетворило Україну на піддослідного кролика, але також і на лабораторію з розробки засобів захисту. Україні вдалося відбити атаки російських хакерів та контратакувати.

Четверта причина. Український інтернет сильно децентралізований, весь сенс інтернету і полягав у створенні комп'ютерної мережі, яка б продовжувала функціонувати навіть у разі тотальної ядерної атаки. Комерційні мережі України продемонстрували свою надійність.

П'ятим фактором є те, що Україна, як і раніше, покладається на технології часів холодної війни у своїх системах озброєння. З усіх боків це недолік, але коли в системах радіолокації замість мікрочипів використовують радіоклапани, вони можуть бути настільки ж невразливі для кібератак, як паровий двигун, що працює на вугіллі.

Наслідки російських кібератак

Наслідки атак російських хакерів у короткостроковій перспективі показують, що приклад України, ймовірно, повторять, йдеться у статті.

«Ми також, ймовірно, не побачимо чистих кібервійн, у яких цифрові атаки замінюють звичайні. Може статися так, що кібератаки відіграватимуть другорядну

роль у руйнуванні інфраструктури, але головну роль — у боротьбі у сфері інформації», — пише автор.

Однак кібервійна має багато переваг, адже атаки проводяться з неймовірною швидкістю, дальністю та точністю. Їхні наслідки можуть бути непомітні, поки не стане надто пізно. З їхньою допомогою можна підставити третю сторону, або втягнути якнайбільше учасників у конфлікт, тим більше його розпалюючи». ***(Ірина Рефагі. РФ не змогла перемогти Україну в кібервійні: 5 причин провалу російських хакерів // Фокус (https://focus.ua/uk/digital/527789-rf-ne-smogla-pobedit-ukrainu-v-kibervoyne-5-prichin-provala-russkih-hakerov). 02.09.2022).***

***

«Фахівці Адміністрації Держспецзв'язку за підтримки Європейського Союзу та американського проєкту від USAID «Кібербезпека критично важливої інфраструктури України» підготували та оприлюднили аналітичний документ «Війна в Україні. Пульс кіберзахисту», в якому узагальнено інформацію про поточний рівень загроз у кіберпросторі на тлі збройної агресії рф та висвітлена діяльність нашої держави щодо забезпечення кіберзахисту. АрміяInform спробує ознайомити наших читачів з основними положеннями зазначеного дослідження та прогнозами стосовно кіберзагроз рф для України та світу.

Щоб розуміти рівень активності агресора в кіберпросторі, варто звернутися до оцінок Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA при Держспецзв'язку, яка протягом шести перших місяців з початку війни проти України (тобто з 24.02.2022 по 24.08.2022) зареєструвала 1123 кібератаки. Окрім наведеної кількості, значна частина атак припала на початок року, ще до широкомасштабного вторгнення. Але вже протягом першого місяця війни Україна зазнала втричі більше кібератак, як порівняти з аналогічним періодом минулого року.

Якщо провести їх структуризацію, то основними напрямами атак хакерів стали державні органи (260 атак) та структури сектору безпеки і оборони України (154). Відповідно, на комерційні організації припало 83 атаки, фінансову сферу — 72.

Щодо мети кібератак, то в 306 випадках здійснювався несанкціонований збір інформації, у 267 — були спроби розмістити шкідливий програмний код, у 149 — спроби втручання у функціонування роботи ресурсів, інші різновиди атак — 401.

Основна мета діяльності російських хакерів із початком війни поступово трансформується. Якщо в січні-березні поточного року кібератаки були спрямовані на комунікації систем державного та військового управління, які мали обмежити ефективність функціонування Сил оборони і державної влади в Україні, то після перших невдач на фронті агресор частково змінив вектор дій і сконцентрував зусилля на завдаванні шкоди цивільному населенню та об'єктам життєзабезпечення. Цей підхід відображає сутність російської армії, яка не звертає уваги на міжнародне право, традиції та правила війни і системно знищує цивільну інфраструктуру (заклади освіти і медицини, інфраструктуру енергетики і транспорту, житлові будинки тощо).

Найбільшу активність від атак російських хакерів відчувають на собі державні та місцеві органи влади, інформаційні ресурси сектору безпеки та оборони,

енергетичний, фінансовий і комерційний сектори, а також ІТ-інфраструктура та транспортна галузь. Наразі хакери все більш активно атакують енергетичний сектор, щоб позбавити українців умов для нормального життя навіть поза окупованими територіями, де вони фізично знищують інфраструктуру населених пунктів.

Зазвичай суб'єкти забезпечення кібербезпеки держави швидко відновлюють роботу систем, які зазнали атак. Зокрема, атаку від 8 квітня на обленерго одного з регіонів було попереджено разом із державами-партнерами та фахівцями самої установи. Крім енергетики, російські хакери також активно атакують транспортну інфраструктуру, щоб завадити евакуації людей, переміщенню країною до більш безпечних міст. Тоді як російські військові намагаються позбавити українських громадян доступу до сервісів зв'язку, фізично атакуючи об'єкти інфраструктури, російські хакери атакують інтернет-провайдерів, наприклад, один із найбільших українських провайдерів — «Укртелеком». Інша група цілей для хакерів — медіа-ресурси та персональні акаунти публічних діячів у соцмережах, що має на меті сприяти поширенню кремлівської пропаганди та фейків.

Слід розуміти, що масштабні та/або комплексні атаки потребують тривалого часу на їхню підготовку. Тому тимчасове зменшення інтенсивності кібератак проти України вказує на підготовчий період з боку агресора до нової хвилі нападів.

З метою протидії ворожій кіберактивності основними суб'єктами забезпечення кібербезпеки держави за провідної ролі Адміністрації Держспецзв'язку здійснювалася взаємодія щодо кіберзахисту з державними органами та представниками критичної інфраструктури, розроблялися необхідні інструкції для користувачів із попередження та розпізнавання кібератак, а також захисту та усунення наслідків. Слід розуміти, що кіберзагрози вже давно перестали бути чимось абстрактним, і поточна ситуація вимагає, щоб кожна людина, насамперед особовий склад Сил оборони, працівники державних установ, підприємств критичної інфраструктури дбали про власну кібербезпеку і пам'ятали, що можуть стати точкою входу для подальшої атаки ворога.

Також Україна продовжує поглиблювати співпрацю з партнерами у сфері кіберзахисту. Адже досвід України в боротьбі з кібератаками російського агресора допомагає не тільки нам, а й нашим партнерам у побудові дієвих національних та міжнародних систем кіберзахисту. Про зазначене свідчить інтерес міжнародної спільноти до інформації від українських фахівців на міжнародних заходах із кібербезпеки. Прикладами є недавня міжнародна конференція команд реагування на комп'ютерні надзвичайні події FIRST і міжнародна конференція з кібербезпеки Black Hat-2022. Україна постійно ділиться з партнерами даними про кіберзброю, яку застосовують російські хакери. З цього напряму в липні поточного року було підписано «Меморандум про взаєморозуміння між Держспецзв'язку та Урядовим офісом Республіки Словенія з інформаційної безпеки у сфері кіберзахисту» та відповідний документ щодо співпраці з Агентством з кібербезпеки та безпеки інфраструктури Департаменту національної безпеки Сполучених Штатів Америки (Cybersecurity and Infrastructure Security Agency). Аналогічно в серпні Україна уклала «Меморандум про взаєморозуміння у сфері кіберзахисту» з Республікою Польща.

Голова Держспецзв'язку Юрій Щиголь: «Розв'язана росією кібервійна проти України показала важливість об'єднання міжнародної спільноти для протидії агресії

в кіберпросторі. Об'єднання зусиль із партнерами стало одним зі стовпів успішного протистояння кібератакам ворога. Цей досвід має бути поширений і стати основою формування колективної системи кіберзахисту демократичного світу. Завдяки підписанню меморандуму ми зможемо значно активніше ділитися здобутими навичками та вміннями з нашими надійними друзями з Польщі».

Очевидно, що наведені міжнародні акти сприяють посиленню спільних дій щодо боротьби зі злочинами в кіберпросторі та роблять обмін досвідом та інформацією про кіберінциденти швидшим і ефективнішим». ***(Тетяна Савченко-Галушко. Як забезпечити захист кіберпростору України на тлі збройної агресії рф // Інформаційне агентство АрміяInform (https://armyinform.com.ua/2022/09/10/yak-zabezpechyty-zahyst-kiberprostoru-ukrayiny-na-tli-zbrojnoyi-agresiyi-rf/). 10.09.2022).***

***

«Українські веб-ресурси та бази даних були захищені від потужних атак, які здійснювалися з території росії та білорусі в перші дні повномасштабного вторгнення, завдяки професіоналізму українських ІТ-фахівців і допомозі іноземних партнерів, зокрема, таких компаній, як Amazon.

Про це розповів Президент Володимир Зеленський під час онлайн-спілкування з керівниками великого американського бізнесу в межах відкриття Нью-Йоркської фондової біржі (NYSE), повідомляє Укрінформ із посиланням на пресслужбу глави держави.

«Збереження наших даних, захист даних – як державних органів, так і приватних компаній – було дуже важливим фундаментальним кроком», – зазначив він.

Зеленський запевнив, що після початку повномасштабного вторгнення рф вистояли навіть ті українські сайти, які зазнали найпотужніших кібератак, зокрема, портал Національного банку, сайти міністерств, Офісу Президента. Також, за його словами, було захищено дані щодо постачання зброї.

Президент пояснив, що це стало можливим завдяки побудові інфраструктури кібербезпеки.

«Ми створили Міністерство цифрової трансформації України. І в кожній державній інституції, у кожному міністерстві, незалежно від того, чим воно займається, сьогодні побудована вертикаль управління, де є спеціальний CEO, заступник із цифровізації. І ця мережа, яку ми побудували, спрацювала», – сказав Президент.

Він зауважив, що в державну структуру були інтегровані найкращі ІТ-фахівці з ринку, а щоб платити їм ринкові зарплати, використовувалися різноманітні грантові програми.

Глава держави також висловив переконання, що інвестиції в Україну є вигідними як для великого бізнесу, так і для нашої країни, оскільки в Україні з'являтимуться нові робочі місця, а бізнес отримає чудові результати завдяки розумним і професійним українським фахівцям.

«Наші люди вільні, креативні, вони вкладають свій інтелект у стартапи», підкреслив Зеленський.

Як зазначили в ОП, напередодні повномасштабної війни українська сторона ухвалила рішення щодо можливості тимчасового зберігання даних за кордоном, і компанія Amazon першою відреагувала на повномасштабне вторгнення й запропонувала Україні необмежений і безкоштовний сервіс для зберігання державних реєстрів. У перші тижні війни 36 українських органів влади перенесли понад 60 своїх критичних реєстрів та систем на ресурси Amazon, серед них – Міністерство внутрішніх справ, Міністерство охорони здоров'я, системи ProZorro, Всеукраїнська школа онлайн тощо. Таким чином компанія Amazon дала змогу створити надійну резервну інфраструктуру для України.

На шостий день війни, 1 березня, російська ракета вдарила по Національному центру резервування даних у середмісті Києва, де зберігаються резервні копії держреєстрів. Але жоден базовий реєстр, за даними Офісу глави держави, та жодна критична держпослуга не були зупинені, а держава стабільно працювала та швидко реагувала на виклики війни. Таким чином функціонування держави було виведене з-під фізичного та віртуального удару російського агресора». ***(Українські сайти витримали найпотужніші кібератаки ворога – Зеленський // Укрінформ (https://www.ukrinform.ua/rubric-technology/3565926-ukrainski-sajti-vitrimali-najpotuznisi-kiberataki-voroga-zelenskij.html). 06.09.2022).***

***

«Група кіберзлочинців, до складу якої входять колишні члени сумнозвісної групи програм-вимагачів Conti, націлена на український уряд і європейські неурядові організації в регіоні, повідомляє Google.

Подробиці містяться в новій публікації в блозі Threat Analysis Group (TAG), команди в Google, яка займається відстеженням кіберактивності, що спонсорується державою.

Оскільки війна в Україні триває понад півроку, кіберактивність, включаючи хактивізм і електронну війну, постійно присутня на задньому плані. Тепер TAG каже, що кіберзлочинці, які шукають прибутку, стають активнішими в цій області.

З квітня по серпень 2022 року TAG стежила за «зростаючою кількістю фінансово вмотивованих загроз, спрямованих на Україну, чия діяльність, здається, тісно пов'язана з підтримуваними російським урядом зловмисниками», – пише Бюро П'єра-Марка TAG. Одного з цих державних суб'єктів уже позначила CERT — національна група реагування на комп'ютерні надзвичайні ситуації України — як UAC-0098. Але новий аналіз TAG пов'язує його з Conti: плідною глобальною бандою програм-вимагачів, яка припинила роботу уряду Коста-Ріки за допомогою кібератаки в травні.

Грунтуючись на багатьох показниках, TAG оцінює, що деякі члени UAC-0098 є колишніми членами кіберзлочинної групи Conti, яка перепрофілює свої методи для націлювання на Україну», — пише Бюро.

Група, відома як UAC-0098, раніше використовувала банківський троян, відомий як IcedID, для здійснення атак програм-вимагачів, але дослідники безпеки Google кажуть, що тепер вони переходять до кампаній, які є «як політично, так і фінансово мотивованими». Відповідно до аналізу TAG, члени цієї групи використовують свій досвід, щоб діяти як посередники початкового доступу —

хакери, які спочатку скомпрометують комп'ютерну систему, а потім продають доступ іншим гравцям, які зацікавлені в експлуатації цілі». ***(Дмитро Сизов. Google: учасники угруповання програм-вимагачів Conti допомагали атакувати Україну // Internetua (https://internetua.com/google-ucsasniki-ugrupovannya-program-vimagacsiv-conti-dopomagali-atakuvati-ukrayinu). 08.09.2022).***

***

«Аналитики Cisco Talos пишут, что русскоязычная хак-группа Gamaredon (она же Primitive Bear, Shuckworm, IronTiden и Callisto) атакует украинские организации с помощью нового инфостилера. Целями этой кампании становятся сотрудники украинских государственных, оборонных и правоохранительных органов.

Эксперты напоминают, что группа Gamaredon известна тем, что использует в своих кампаниях только инструменты собственной разработки, включая вредоносные скрипты, бэкдоры и инфостилеры.

В рамках новой кампании, которая началась в августе 2022 года и по-прежнему активна, хакеры стали применять новый инструмент для хищения информации, который способен извлекать с компьютеров жертв определенные типы файлов, а также развертывать дополнительные пейлоады.

«Это новый инфостилер, который Gamaredon ранее не использовала. Мы подозреваем, что это новый компонент семейства бэкдоров Giddome, но в настоящее время не можем это подтвердить», — пишут в Cisco Talos.

Новая малварь пока не получила собственного имени, но известно, что она имеет четкие инструкции по краже файлов со следующими расширениями:.doc,.docx,.xls,.rtf,.odt,.txt,.jpg,. jpeg,.pdf,.ps1,.rar,.zip,.7z и.mdb. Новый стилер Gamaredon может похищать файлы с подключенных устройств (локальных и удаленных), создавая для каждого украденного файла свой POST-запрос с метаданными и его содержимым.

Эксперты говорят, что этот инфостилер распространяется с помощью фишинговых писем, в которых содержатся документы Microsoft Office с вредоносными макросами VBS. Код VBS скрыт в удаленных шаблонах и выполняется при открытии документа, после чего загружает RAR-архив с LNK-файлами.

Файлы LNK предназначены для запуска mshta.exe, с целью загрузки и парсинга удаленного XML-файла, выполняющего вредоносный PowerShell-скрипт, который Gamaredon ранее уже использовала в своих шпионских кампаниях.

Другой скрипт PowerShell загружается и выполняется с целью сбора данных о зараженной системе (имя компьютера, VSN, скриншот закодированный base64) и последующей отправки этой информации на удаленный сервер». ***(Мария Нефёдова. Хак-группа Gamaredon использует новую малварь против украинских организаций // xakep (https://xakep.ru/2022/09/16/gamaredon-infostealer/). 16.09.2022).***

***

«Українські хакери зламали сайт одної з найбільших російських енергомережевих компаній «Мособленерго» та портал «Крым для россиян»…

На сайті Мособленерго 16 вересня з'явилося зображення охопленого вогнем Кремля. На тлі цієї масштабної пожежі нібито прогулюється секретар РНБО Олексій Данілов. Після появи такої ілюстрації сайт компанії припинив бути доступним.

Інформаційний портал «Крым для россиян» після 16 вересня подає дані про втрати російських окупантів в Україні. Раніше там публікували інформацію про відпочинок на тимчасово окупованому півострові…» ***(«Данілов на тлі палаючого Кремля». Українські хакери зламали сайт Мособленерго // MediaSapiens (https://ms.detector.media/kiberbezpeka/post/30273/2022-09-17-danilov-na-tli-palayuchogo-kremlya-ukrainski-khakery-zlamaly-sayt-mosoblenergo/). 17.09.2022).***

***

«Українська ІТ-армія повідомила, що зламала сайт так званої приватної військової компанії «Вагнер», яка набирає для війни в Україні найманців серед в'язнів російських виправних установ.

«Всі персональні дані найманців у нас! На кожного ката, вбивцю та ґвалтівника чекає сурове покарання. Помста неминуча!» – йдеться в повідомленні ІТ-армії…» ***(Українська ІТ-армія зламала сайт ПВК «Вагнер» // MediaSapiens (https://ms.detector.media/kiberbezpeka/post/30288/2022-09-20-ukrainska-it-armiya-zlamala-sayt-pvk-vagner/). 20.09.2022).***

***

«Кремль планує здійснити масовані кібератаки на об'єкти енергетичної галузі України. Росіяни також планують збільшити кількість DDoS-атак на установи Польщі та країн Балтії.

Таку інформацію оприлюднила пресслужба Головного управління розвідки Міноборони України у понеділок, 26 вересня.

«Насамперед удар буде спрямований на підприємства енергетичної галузі. Цим ворог спробує посилити ефект ракетних ударів по об'єктах електрозабезпечення, насамперед у східному та південному регіонах України», - йдеться у повідомленні.

У розвідці вважають, що росія намагається таким чином уповільнити контрнаступ Збройних сил України.

ГУР зазначає, що росіяни під час проведення нових кіберударів використовуватимуть досвід кібератак на енергосистеми України 2015 та 2016 років.

«Також кремль планує збільшити інтенсивність DDoS-атак на критичну інфраструктуру найближчих союзників України, насамперед Польщі та країн Балтії», - додали у розвідці…» ***(РФ готує нові кібератаки на об'єкти критичної інфраструктури України – ГУР // Слово і Діло (https://www.slovoidilo.ua/2022/09/26/novyna/suspilstvo/rf-hotuye-novi-kiberataky-obyekty-krytychnoyi-infrastruktury-ukrayiny-hur). 26.09.2022).***

***

«Западные страны помогли Украине организовать киберзащиту, которая лишила Россию преимущества в киберпространстве и снизила число успешных хакерских атак на страну, сообщает The Wall Street Journal со ссылкой на источники среди бывших и нынешних западных чиновников.

После начала войны Украина в основном избежала серьезных последствий от действий хакеров, хотя до вторжения регулярно страдала от таких кибератак. Кибербезопасность страны была усилена в том числе благодаря помощи со стороны США, считают западные разведчики и аналитики. Вашингтон передавал Украине разведданные, обучал специалистов по кибербезопасности и помогал укреплять защиту критической инфраструктуры от хакерских атак.

В прошлом году США направили в союзные страны, в том числе в Украину, своих экспертов по цифровой безопасности. Они должны были выявить потенциальные угрозы для важнейших компьютерных сетей и обучить коллег из других стран способам защиты. Киберкомандование вооруженных сил США в августе сообщило, что сотрудники ведомства успешно завершили 35 задач в 18 странах, включая Хорватию, Эстонию, Литву, Черногорию и Северную Македонию.

Зампредседателя Государственной службы спецсвязи и защиты информации Украины Виктор Жора подтвердил важность роли США и других союзников в успехах Украины. Украинские чиновники, как пишет WSJ, считают, что Россия уже использовала большую часть своих кибервозможностей.

По мнению аналитиков, российским хакерам, одним из самых опытных в мире, не удалось переломить ход войны. Однако списывать российских хакеров, по мнению действующих и бывших сотрудников западных служб безопасности, тоже не стоит. Эксперты напоминают, что российские хакеры изобретательны, терпеливы и дисциплинированы.

До войны Украина была более беззащитна перед кибератаками: до вторжения российские хакеры атаковали сайты украинского правительства, а 24 февраля атака вывела из строя тысячи модемов в Украине, нарушив линии связи между вооруженными силами.

С началом войны активность российских хакеров усилилась. Так, например, кибератакам подверглись Литва после частичного запрета на транзит в Калининград, а также Эстония и Латвия после демонтажа советских памятников». ***(Россия лишилась преимущества в киберпространстве перед Украиной // Меридиан Севастополь (https://meridian.in.ua/news/69231.html). 06.09.2022).***

***

«Кіберскладова є важливим елементом у війні України проти росії. Про це заявив секретар Ради національної безпеки і оборони України Олексій Данілов.

Він наголосив, що на початку війни усі суб'єкти забезпечення кібербезпеки України виступили єдиним фронтом, що допомогло відбити російських агресорів у кіберпросторі.

За словами Данілова, ефективність кібербезпеки та відбиття кібератак в умовах воєнного стану полягає у максимальній координації та командній роботи.

Міністр цифрової трансформації України Михайло Федоров своєю чергою зазначив, що за останні пів року рівень координації між суб'єктами гарантування кібербезпеки суттєво зріс.

Федоров відзначив оперативність ухвалення законодавчих рішень для розміщення бекапів баз даних у хмарних сервісах за кордоном, активізацію роботи «червоних команд» тощо.

Натепер українські фахівці завершують розробляти індикатори виконання Стратегії кібербезпеки України, до чого залучили представників СБУ, Держспецзв'язку, Нацполіції, НБУ, Мінцифри, Міноборони, Генерального штабу ЗСУ, розвідувальних органів, а також Національного інституту стратегічних досліджень.

Також в Україні розробили Порядок взаємодії суб'єктів гарантування кібербезпеки під час реагування на кіберінциденти/кібератаки. Зокрема, документ визначає:

принципи, на яких ґрунтуватиметься застосування цього порядку;

рівні критичності кіберінцидентів/кібератак;

алгоритм взаємодії під час реагування на кіберінциденти/кібератаки різного рівня критичності». ***(Ірина Маринюк. Кіберскладова цієї війни важлива: в Україні розробляють стратегію кібербезпеки // speka.media (https://speka.media/n3kiberskladova-ciyeyi-vijni-vazhliva-v-ukrayini-rozroblyayut-strategiyu-kiberbezpeki114-v567np). 23.09.2022).***

***

«Восьмий пакет санкцій Євросоюзу проти росії потенційно може включати обмеження цін на російську нафту, додаткові списки підсанкційних осіб, а також заходи, спрямовані на російські галузі інформаційних технологій, кібербезпеки та програмного забезпечення.

Про це повідомляє Financial Times із посиланням на джерела.

Як пише видання, «яструби» в ЄС наполягають на жорстких заходах проти росії, у тому числі на виключення ще більшої кількості банків із Swift та заборони на імпорт алмазів.

Країни, у тому числі Польща та балтійські, вимагають заходів, націлених на предмети розкоші та російські галузі інформаційних технологій, кібербезпеки та програмного забезпечення.

При цьому офіційні особи кажуть, що важко знайти консенсус між усіма 27 державами-членами, а Угорщина взагалі заявила, що проти будь-яких нових санкцій. Головна мета Єврокомісії – проштовхнути угоду G7 щодо обмеження цін на російську нафту.

За словами джерел, після ЄС мають обговорити проєкт нових санкцій наступного тижня…» ***(Нові санкції Євросоюзу проти росії можуть торкнутися сфер IT та кібербезпеки – FT // Слово і Діло (https://www.slovoidilo.ua/2022/09/23/novyna/polityka/novi-sankcziyi-yevrosoyuzu-proty-rosiyi-mozhut-torknutysya-sfer-it-ta-kiberbezpeky-ft). 23.09.2022).***

***

«После вторжения 24 февраля Россия ведет продолжительную злонамеренную киберкампанию против Украины и ее союзников, но ее отсутствие успеха показывает, что можно защититься от кибератак, даже от самых изощренных и настойчивых злоумышленников, говорится в сообщении британской службы кибербезопасности. главный.

«Как бы они ни старались, российские кибератаки просто не оказали должного воздействия», — заявила Линди Кэмерон, генеральный директор Национального центра кибербезопасности (NCSC) — киберподразделения GCHQ — выступая в Chatham House в Лондоне.

«Но если украинская киберзащита преподает нам более широкий урок — для военной теории и не только — это то, что в кибербезопасности защитник имеет значительную свободу действий. Во многих отношениях вы можете выбирать, насколько вы можете быть уязвимы для атак».

В преддверии и после вторжения в Украину страна подверглась серии кибератак, приписываемых России. К ним относятся распределенные атаки типа «отказ в обслуживании» (DDoS) против правительства и финансового сектора Украины, а также кампании по удалению вредоносных программ, предназначенные для уничтожения систем, делая их непригодными для использования.

Это были не первые наступательные кибератаки, связанные с российским государством, направленные против Украины; атаки ранее приводили к отключению электроэнергии зимой 2015 и 2016 годов. Затем, в 2017 году, Россия запустила атаку вредоносного ПО NotPetya wiper против Украины, но воздействие распространилось дальше, причинив ущерб на миллиарды долларов по всему миру.

По словам Кэмерона, после вторжения «мы наблюдаем очень серьезный конфликт в киберпространстве — вероятно, самую продолжительную и интенсивную киберкампанию за всю историю». Но она также указала на безуспешность этих кампаний благодаря усилиям украинских киберзащитников и их союзников.

«Эта деятельность предоставила нам наиболее четкую демонстрацию того, что мощную и эффективную киберзащиту можно создать даже против такого хорошо подготовленного и обеспеченного ресурсами противника, как Российская Федерация».

Кэмерон утверждал, что это не только дает уроки о том, что страны и их правительства могут сделать для защиты от кибератак, но также дает организациям уроки о том, как защититься от инцидентов, будь то поддерживаемые государством кампании, атаки программ-вымогателей или другие злонамеренные кибератаки. операции.

«Главное в этом — приверженность долгосрочной устойчивости», — сказал Кэмерон. «Повышение устойчивости означает, что нам не обязательно знать, где и как угроза проявится в следующий раз. Вместо этого мы знаем, что большинство угроз не смогут пробить нашу защиту. И когда они это сделают, мы сможем быстро и полностью восстановиться».

NCSC ранее предлагал организациям работать с повышенным уровнем угроз и дал рекомендации, которым следует следовать, чтобы помочь защититься от кибератак или побочного ущерба в результате широкомасштабных кибератак.

Эти рекомендации, которые Кэмерон повторил в Chatham House, включают в себя проверку того, чтобы все программное обеспечение было обновлено с последними исправлениями безопасности, проверка правильности работы резервных копий и наличие плана реагирования на инциденты, поскольку кибератаки продолжают представлять серьезную угрозу.

«Могут быть организации, которые начинают думать: «А нужно ли это?» как и в Великобритании, у нас не было серьезных инцидентов, связанных с войной в Украине. Мой ответ — решительное «да», — сказал Кэмерон.

«Британские организации — и их сетевые защитники — должны быть готовы к этому периоду повышенной готовности, чтобы быть с нами в течение длительного времени. По всей Великобритании нам нужно сосредоточиться на создании долгосрочной устойчивости. Как это сделали украинские защитники», - добавила она». ***(Danny Palmer. Russian hackers' lack of success against Ukraine shows that strong cyber defences work, says cybersecurity chief // ZDNET (https://www.zdnet.com/article/russian-hackers-lack-of-success-against-ukraine-shows-strong-cyber-defences-work-says-cybersecurity-chief/). 29.09.2022).***

***

«Служба военной разведки Украины предупредила сегодня, что Россия планирует «массированные кибератаки», нацеленные на критическую инфраструктуру Украины и ее союзников.

По данным Главного управления разведки Министерства обороны Украины (ГУР МО), эта грядущая «массированная» волна атак, скорее всего, будет направлена на разрушение и уничтожение объектов и учреждений энергетической отрасли.

«Кремль планирует провести массированные кибератаки на критическую инфраструктуру украинских предприятий и объектов критической инфраструктуры союзников Украины», — предупредила спецслужба.

«В первую очередь удар будет направлен на энергетику. В операциях будет использован опыт кибератак на энергосистемы Украины в 2015 и 2016 годах».

Вероятная цель российских кибератак — затормозить продолжающееся наступление украинской армии и усилить разрушительный эффект ракетных ударов по украинским объектам энергоснабжения в восточных и южных регионах.

«Кремль также намерен увеличить интенсивность DDoS-атак на критическую инфраструктуру ближайших союзников Украины, в первую очередь Польши и стран Балтии», — добавили в HUR MO.

Это предупреждение следует за июльским заявлением Совета Европейского Союза о том, что российские группы угроз, которые все чаще атакуют «основные» организации по всему миру, могут привести к потенциальной эскалации и рискам распространения.

В феврале CISA и ФБР также заявили в совместном бюллетене, что атаки вредоносного ПО Wiper, нацеленные на Украину, могут легко распространиться на цели из других стран.

Их совместные рекомендации также содержат рекомендации и меры, которые следует принимать в рамках сетевой архитектуры, базовых показателей безопасности и постоянного мониторинга для защиты от таких атак.

Группа анализа угроз Google (TAG) добавила в конце марта, что фишинговые атаки на военные объекты НАТО и Европы были организованы российской хакерской группой COLDRIVER.

Два месяца спустя США, Великобритания и ЕС совместно обвинили Россию в координации масштабной кибератаки, которая поразила ориентированную на потребителя услугу спутниковой широкополосной связи KA-SAT в Украине 24 февраля, за час до того, как Россия вторглась в Украину с помощью данных AcidRain, уничтожающих вредоносное ПО.

Президент США Джо Байден предупредил в июле 2021 года, что кибератаки, ведущие к серьезным нарушениям безопасности, могут спровоцировать «настоящую перестрелку». Это заявление было сделано через месяц после того, как НАТО заявило [PDF], что кибератаки можно сравнить с «вооруженными атаками». (в некоторых случаях)». ***(Sergiu Gatlan. Ukraine warns allies of Russian plans to escalate cyberattacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ukraine-warns-allies-of-russian-plans-to-escalate-cyberattacks/). 26.09.2022).***

***

«У нас – один ворог, і цей ворог добре підготовлений до наступних ударів. Він готовий здійснювати кібератаки на демократичні країни. Про це сьогодні, виступаючи на міжнародній конференції «Формуючи кібербезпеку», заявив заступник голови Держспецзв'язку Олександр Потій.

Він зауважив, що нинішнє зниження атак можна пояснити «періодом підготовки» до майбутніх. Щоб ефективно протистояти російським хакерам, країни ЄС і НАТО повинні зосередити зусилля на посиленні кіберстійкості та запобіганні агресії у кіберпросторі. Важливо посилювати групи швидкого реагування на такі інциденти, працювати разом над стандартами, будувати взаємовигідні партнерські відносини та спільні команди протидії кіберагресії.

«Але головною метою для всіх нас є рівень обізнаності про загрози. Цифрова безпека та кібергігієна мають бути частиною повсякденного життя як кожного пересічного громадянина, так і кожного керівника. Стандарти безпеки – це межа між нами та ворогом. І ця межа є в будь-якому смартфоні, комп'ютері, реєстрі та системі компанії», – підкреслив заступник голови Держспецзв'язку.

За його словами, з першої у світі кібервійни можна засвоїти кілька важливих уроків.

Кібератаки на Україну слугують підтримкою російських воєнно-політичних операцій. Злочинні угруповання добре скоординовані спецслужбами: ГРУ, ФСБ, російський генштаб.

Викрадення грошей і викуп не є справжніми цілями кібератак. Ворог має намір збирати інформацію (як про державну, так і про приватну інфраструктуру, а також про пересічних громадян). Він працює на знищення інформаційної інфраструктури, на поширення паніки та недовіри до влади серед людей.

Крім того, російська федерація свідомо атакує цивільну інфраструктуру та цивільні цілі». ***(Військові хакери з рф готові здійснювати кібератаки на демократичні країни // Компьютерное Обозрение (https://ko.com.ua/vijskovi_hakeri_z_rf_gotovi_zdijsnyuvati_kiberataki_na_demokratichni_krayini_142201). 28.09.2022).***

***

«Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка діє при Держспецзв'язку, оприлюднила рекомендації щодо дослідження десятків цільових атак, спрямованих на виведення з ладу інформаційно-комунікаційних систем та порушення конфіденційності інформації, що в них обробляється.

Фахівці команди визначили слабкі місця у використанні програмного забезпечення, які є найбільш вразливими для компрометації та можуть призвести до атак «вглиб» комп'ютерної мережі, викрадення паролів привілейованих облікових записів та порушення штатного режиму функціонування елементів інформаційно-комунікаційної системи.

Враховуючи результати досліджень, CERT-UA звертається до керівників установ із рекомендацією проведення відповідних безпекових заходів: перевірка доступних із мережі інформаційних систем, перевірка IP-адрес щодо асоційованих вразливостей.

Детальні рекомендації доступні на порталі CERT-UA, до команди також можна звертатися за консультативно-методичною та практичною допомогою, зокрема з перевірки вебресурсів на наявність вразливостей.

«Дотримання цих рекомендацій критично важливе у період воєнного стану, оскільки кордон безпеки у протистоянні злочинним діям агресора пролягає в кожному комп'ютері, кожному смартфоні та за кожним безпековим контуром підприємства чи організації. Дотримання правил і стандартів є внеском кожного з нас в безпеку країни. А ризик нових атак залишається надзвичайно високим від 14 січня, першої масованої кібератаки на Україну з боку агресора», – зазначив речник ДССЗЗІ Володимир Кондрашов.

CERT-UA нагадує, що відповідальність за забезпечення захисту інформації в системі покладається на власника системи. Та рекомендує керівникам підприємств, установ і організацій взяти питання щодо впровадження зазначених невідкладних заходів під особистий контроль». ***(Підприємства, установи і організації мають терміново посилити кіберзахист – рекомендації CERT-UA // Офіційний сайт Кіберполіції України (https://cyberpolice.gov.ua/news/pidpryyemstva-ustanovy-i-organizacziyi-mayut-terminovo-posylyty-kiberzaxyst--rekomendacziyi-cert-ua-8753/). 29.09.2022).***

***

«З початку 2022 року кіберфахівці Служби безпеки України знешкодили 35 ботоферм. Про це начальник Департаменту кібербезпеки СБУ Ілля Вітюк заявив в ефірі національного телемарафону.

«З початку року ми припинили функціонування вже 35 ботоферм. Тобто департамент кібербезпеки системно протидіє інформаційній агресії російської федерації, не допускаючи розхитування суспільно-політичної ситуації в нашій державі», – підкреслив він.

Зокрема, тільки за останні кілька днів викрито ботоферми на Київщині, Одещині та у столиці, які серед іншого дискредитували українських захисників, поширювали панічні настрої та розганяли російські наративи.

За словами Іллі Вітюка, ботоферми зазвичай створюються, як шахрайський інструмент масштабування інформаційного впливу на певні аудиторії.

При цьому відповідальність за такий злочин має бути посилена.

Адже на сьогоднішні день створення ботоферми класифікується, як несанкціоноване втручання в роботу електронно-обчислювальних мереж (ст. 361 Кримінального кодексу України) і карається штрафом або ж позбавленням волі від 2 до 6 років максимум.

Водночас чимало ботоферм працюють на російські спецслужби. А отже кваліфікувати такі дії вже варто, як пособництво державі-агресору чи й державну зраду, що тягне за собою значно вищий рівень відповідальності.

«Наші спеціалісти напрацьовують відповідні ініціативи та зміни до законодавства. Ми вважаємо, що необхідно виділити питання кваліфікації дій – зокрема, створення та функціонування бото- і тролеферм – в окремий склад злочину з огляду на його суспільну небезпеку, особливо у військовий час», – зазначив Ілля Вітюк.

Він нагадав, що кібервійна для України розпочалася ще у 2014 році, і рф використовує в ній різноманітні інструменти впливу.

Наприклад, нещодавно викрита СБУ мільйонна ботоферма, організована політтехнологом-громадянином рф, який переїхав в Україну, використовувалася не лише окремими політичними силами в нашій державі, а й російськими спецслужбами». ***(Артем Сереженок. СБУ знешкодила 35 ботоферм та ініціює посилення відповідальності за їх створення // Internetua (https://internetua.com/sbu-zneshkodila-35-botoferm-ta-iniciuaye-posilennya-vidpovidalnosti-za-yih-stvorennya). 07.09.2022).***

***

«Служба безпеки нейтралізувала хакерське угруповання, яке діяло в інтересах країни-агресора у Львові.

Зловмисники зламували активні облікові записи інтернет-користувачів з України та Євросоюзу, отримуючи доступ до персональних даних громадян.

Цю конфіденційну інформацію вони продавали через анонімну платформу «Даркнет», а гроші отримували на заборонені в нашій державі електронні платіжні системи ЮMoney, Qiwi та WebMoney.

За попередніми даними, хакери продали орієнтовно 30 млн акаунтів і одержали «прибуток» у розмірі майже 14 млн грн.

Їхніми «оптовими клієнтами» були прокремлівські пропагандисти. Саме вони використовували одержані установчі дані українських та іноземних громадян для поширення фейкових «новин» з фронту та створення панічних настроїв. Метою таких маніпуляцій була масштабна дестабілізація в країнах.

Також встановлено, що зламані акаунти використовували нібито від імені пересічних людей для поширення дезінформації щодо суспільно-політичної ситуації в Україні та ЄС.

За даними слідства, до складу угруповання входило декілька хакерів зі Львова. Спеціалізоване комп'ютерне обладнання вони встановили у своїх помешканнях.

Зловмисники «проникали» до чужих акаунтів через шкідливе програмне забезпечення.

Під час обшуків правоохоронці виявили:

жорсткі магнітні диски з персональними даними громадян;

комп'ютерну техніку, мобільні телефони, сім-карти та флеш-накопичувачі з доказами незаконної діяльності.

Наразі організатору повідомлено про підозру за ч. 1 ст. 361-2 (несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) Кримінального кодексу України.

Тривають слідчо-оперативні дії для притягнення до відповідальності всіх винних осіб.

Заходи з викриття злочинів проводили співробітники кіберпідрозділу СБУ Львівської області спільно з Національною поліцією за процесуального керівництва Галицької окружної прокуратури». ***(СБУ нейтралізувала хакерське угруповання, яке «зламало» майже 30 млн акаунтів громадян України та ЄС // Служба безпеки України (https://ssu.gov.ua/novyny/sbu-neitralizuvala-khakerske-uhrupovannia-yake-zlamalo-maizhe-30-mln-akauntiv-hromadian-ukrainy-ta-yes). 23.09.2022).***

***

«…Служба безпеки України повідомила про нейтралізацію хакерського угруповання, яке діяло у Львові в інтересах країни-агресора.

За даними СБУ, конфіденційну інформацію зловмисники продавали через анонімну платформу «Даркнет», а гроші отримували на заборонені в Україні електронні платіжні системи ЮMoney, Qiwi та WebMoney.

За попередніми даними, хакери продали орієнтовно 30 млн акаунтів і одержали за це майже 14 млн грн.

«Їхніми «оптовими клієнтами» були прокремлівські пропагандисти. Саме вони використовували одержані установчі дані українських та іноземних громадян для поширення фейкових "новин" з фронту та створення панічних настроїв. Метою таких маніпуляцій була масштабна дестабілізація в країнах», – повідомляє СБУ.

Також встановлено, що зламані акаунти використовували нібито від імені пересічних людей для поширення дезінформації щодо суспільно-політичної ситуації в Україні та ЄС.

За даними слідства, до складу угруповання входило декілька хакерів зі Львова. Спеціалізоване комп'ютерне обладнання вони встановили у своїх помешканнях.

Зловмисники «проникали» до чужих акаунтів через шкідливе програмне забезпечення.

Під час обшуків правоохоронці виявили жорсткі магнітні диски з персональними даними громадян, комп'ютерну техніку, мобільні телефони, сім-карти та флеш-накопичувачі з доказами незаконної діяльності.

Організатору повідомлено про підозру за ч. 1 ст. 361-2 (несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) Кримінального кодексу України». ***(СБУ викрила хакерів, які «зламали» майже 30 млн акаунтів в Україні та ЄС та продали їх Росії // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/30310/2022-09-23-sbu-vykryla-khakeriv-yaki-zlamaly-mayzhe-30-mln-akauntiv-v-ukraini-ta-ies-ta-prodaly-ikh-rosii/). 23.09.2022).***

***

«Українські кібербійці паралізували понад 4000 російських онлайн-ресурсів за 2 тижні.

Українська ІТ-армія продовжує розхитувати економіку ворога та деморалізувати росіян на цифровому фронті. Про це повідомляє Міністерство цифрової трансформації України.

Так, з 12 до 25 вересня через дії ІТ-армії призупинили роботу:

Сайт приватної військової компанії Вагнера, чиї найманці воюють в Україні. Були отримані всі дані, які зберігалися на сайті. «На кожного ката, вбивцю та ґвалтівника чекає суворе покарання», - запевнили в Мінцифри.

Ресурси організації «Молодая гвардия Единой Росии». ІТ-армія отримала списки путіністів, які були або є на окупованих територіях, допомагають приховувати воєнні злочини та проводити незаконні референдуми.

Портал «Госуслуги». Через атаку на портал росіяни не могли отримати бажані послуги, адже з ресурсом пов'язані сотні сторонніх сервісів, які залучені в державних, економічних та військових сферах.

Сайти для пошуку роботи. На таких сайтах Міністерство оборони Росії часто публікує вакансії для військових. Тепер для росіян жодна вакансія недоступна, як і самі портали.

Військторгі РФ. Через це росіяни не могли замовити необхідне спорядження для своїх солдатів-вбивць, які продовжують вести війну в Україні.

Сайти з продажу автоінструментів. ІТ-армія перекрила не тільки можливість росіянам продавати у РФ контрабанду у вигляді інструментів для авто з Європи, а і купувати необхідне автоприладдя своїм військовим на фронт.

Комерційний банк «Открытие». DDoS-атака на інфраструктуру банку заблокувала росіянам можливість користуватися банківськими послугами онлайн». ***(Українська ІТ-армія зламала тисячі російських ресурсів // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/30328/2022-09-26-ukrainska-it-armiya-zlamala-tysyachi-rosiyskykh-resursiv/). 26.09.2022).***

***

Міжнародне співробітництво у галузі кібербезпеки

Заступник голови Держспецзв'язку Олександр Потій зустрівся із командувачем Військ оборони кіберпростору Польщі Каролем Молендою. Це перша зустріч сторін, спрямована на реалізацію меморандуму про взаєморозуміння у сфері кіберзахисту, підписаного 22 серпня між Урядами України та Польщі.

Під час зустрічі, у якій також взяли участь експерти з кібербезпеки та міжнародного співробітництва, обговорили роль кожного органу в системах оборони країн, їхню сферу діяльності та зони відповідальності, роботу українських та польських команд реагування на кіберінциденти, а також загальну екосистему кібербезпеки та платформ обміну інформацією.

«Експертний досвід, який має у своєму розпорядженні Україна, є неоціненним для спільної побудови та розвитку можливостей у сфері активного захисту від кіберзагроз», – зазначив генерал Кароль Моленда.

За словами Олександра Потія, об'єднання зусиль із партнерами – запорука успішного протистояння ворожим кібератакам. Жорстока війна, яку розв'язала росія, триває на території України. Але кіберпростір не має кордонів, і російські хакери атакують не тільки нашу державу, а й інші країни – усіх, хто підтримує українську незалежність, демократичні цінності.

«Об'єднання кіберпотенціалів Польщі та України, безсумнівно, принесе користь обом нашим державам та народам. Це дозволить нам побудувати безпечний кіберпростір, разом протистояти кіберагресії», – підкреслив заступник голови Держспецзв'язку.

Співпраця України та Польщі щодо протидії загрозам у кіберпросторі та побудові надійного захисту від кібератак буде і надалі поглиблюватися. Це й обмін інформацією та досвідом, і проведення спільних навчань, тренінгів, консультацій, а також інші заходи, які дозволять підсилити кіберспроможність обох країн.

«Ми розпочинаємо напрацювання конкретних планів для вирішення нових завдань і досягнення нових результатів. Будемо наповнювати українсько-польський меморандум конкретними проєктами та програмами», – зазначив Олександр Потій». ***(Україна поглиблює співпрацю з Польщею у сфері кібербезпеки // Урядовий кур'єр (http://ukurier.gov.ua/uk/news/ukrayina-pogliblyuye-spivpracyu-z-polsheyu-u-sferi/). 01.09.2022).***

***

«Україна стала учасницею програми Європейського Союзу «Цифрова Європа». У межах ініціативи наша держава отримає доступ до фінансування цифрових проєктів на 6 мільярдів євро, повідомляє Міністерство цифрової трансформації в Telegram.

«Україна долучилася до програми «Цифрова Європа». Це наближає нас до цифрового безвізу з ЄС», – йдеться в повідомленні.

Зазначена ініціатива була створена для пришвидшення цифрової трансформації Євросоюзу. Завдяки ній, наша країна зможе отримати фінансування в низці напрямів:

Високопродуктивні комп'ютери;

Штучний інтелект, дані й хмарні послуги;

Цифрові навички;

Використання цифрових технологій в економіці й суспільстві.

Програма також передбачає надання коштів у галузі кібербезпеки, однак цей напрямок є закритим для держав, що не входять до складу ЄС.

Таким чином, доступним для України стане фінансування за кількома напрямами на суму 6 млрд євро, які виділятимуться впродовж семи років. Загальний же фонд «Цифрової Європи» складає 7,6 млрд євро.

У Мінцифрі уточнили, що восени на сайті Digital Europe розмістять робочі програми й конкурсні пропозиції, а також подробиці подання заявок для участі…» ***(Україна долучилася до програми «Цифрова Європа»: що зможе отримати держава // Дзеркало тижня. Україна (https://zn.ua/ukr/TECHNOLOGIES/ukrajina-doluchilasja-do-prohrami-tsifrova-jevropa-shcho-zmozhe-otrimati-derzhava.html). 05.09.2022).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Внезапный переход на удаленную работу, вызванный глобальной пандемией, вызвал множество изменений в отношении компаний, управляющих своей деятельностью. ИТ-инфраструктура оказалась настоящей проблемой, поскольку большинство работников, работающих дома, не имели бы доступа к тем же высококлассным средствам кибербезопасности, которые есть у их работодателей в офисе.

Удаленная работа сделала необходимым расширение использования облачных серверов, потому что это может потенциально упростить совместную работу. Несмотря на то, что это так, это также принесло множество проблем, поскольку все было учтено и принято во внимание. Согласно данным, которые были только что опубликованы Atlas VPN, кажется, что 41% компаний, которые пострадали от кибератаки в прошлом году, сообщили, что источником был их облачный сервер.

После всего сказанного важно отметить, что это представляет собой увеличение на десять процентов в годовом исчислении. Злоумышленники явно

наслаждаются слабой безопасностью, предлагаемой облачными серверами в наши дни, и увеличение объема атак является свидетельством этого.

Следует также отметить, что деловая электронная почта также была частым источником кибератак. 40% компаний заявили, что скомпрометированные электронные письма привели к обходу их протоколов безопасности, что просто показывает, что киберпреступники имеют в своем арсенале широкий набор инструментов.

Третьим наиболее распространенным каналом, через который проводятся кибератаки, являются корпоративные серверы. Это противоречит представлению о том, что удаленная работа виновата в росте киберпреступности. Корпорации явно недостаточно заботятся о своей безопасности, и подобные данные доказывают, что им нужно привести свои дела в порядок.

Действительно, мобильные устройства, принадлежащие сотрудникам, использовались в 31% кибератак, поэтому даже официальные устройства с загруженными на них протоколами безопасности не защищены от этих атак. Необходимо проделать дополнительную работу, чтобы держать оборону от киберпреступлений против юридических лиц». ***(Zia Muhammad. 41% of Cyber Attacks Are Now Done Through Cloud Servers, New Data Reveals // Digital Information World (https://www.digitalinformationworld.com/2022/09/41-of-cyber-attacks-are-now-done.html). 07.09.2022).***

***

Світові тенденції в галузі кібербезпеки

«…Интернет стал еще более неотъемлемой частью мировой экономики, что вызвало необходимость повышения кибербезопасности в ответ на быстрое развитие технологий и методов взлома. Это открывает компаниям возможность привлекать новые венчурные инвестиции путем разработки более совершенных инструментов кибербезопасности.

Однако кибербезопасность по-прежнему находится в центре внимания инвесторов, поэтому стоит поближе познакомиться с отраслью, чтобы увидеть, на что, скорее всего, будут потрачены средства венчурного капитала.

Киберпреступность опережает экономический спад: великий спад или рыночная стабилизация?

Cybersecurity Ventures прогнозирует, что в 2021 году мировая экономика потеряет около 6 триллионов долларов из-за киберпреступности. Если мы сравним эту цифру с мировым ВВП, она станет третьей по величине мировой экономикой после США и Китая. Текущие прогнозы предполагают 15% AGR для киберпреступности. Это означает, что компании, вероятно, будут готовы заплатить меньше, чем прогнозируемые 6 триллионов долларов, за более эффективные меры кибербезопасности, чтобы предотвратить будущие убытки.

В конце 2021 года глобальный рынок кибербезопасности оценивался чуть менее чем в 185 миллиардов долларов, и ежегодные показатели финансирования инвестиций киберкомпаний также неуклонно растут. Двузначные оценки AGR

киберпреступности в сочетании с этими показателями роста подтверждают идею о том, что кибербезопасность готова занять большую долю рынка.

К сожалению, правда заключается в том, что киберпреступность в настоящее время является одним из самых прибыльных нелегальных рынков. Он превратился из молодых хакеров-одиночек в полноценные синдикаты, которые вкладывают миллионы в эти незаконные операции. Хотя спонсируемая государством кибервойна является щекотливой темой, факт остается фактом: страны теперь могут прямо или косвенно финансировать хакеров для проведения кибератак, которые стоят меньше и достигают большего, чем традиционные военные операции.

Беспрецедентный уровень передовых технологий киберпреступности означает, что индустрия кибербезопасности должна продолжать внедрять инновации быстрыми темпами, чтобы не отставать. Есть несколько многообещающих направлений кибербезопасности для стартапов, и я думаю, что именно здесь последует финансирование.

Отрасли, за которыми стоит следить

Компании, занимающиеся кибербезопасностью, привлекли 11 миллиардов долларов в 2020 году (платный доступ) и 26 миллиардов долларов в 2021 году. К концу 2022 года оценка финансирования составляет 21 миллиард долларов, и ожидается значительный рост по сравнению с 2020 годом. Это увеличение в значительной степени связано с несколькими важные новые тенденции, и я полагаю, что их рост заинтересует инвесторов:

1. Искусственный интеллект

Недавний опрос показал, что более половины специалистов по ИТ-безопасности перегружены объемом получаемых предупреждений о безопасности и не могут уверенно расставлять приоритеты и реагировать на них. Чтобы решить эту проблему, стартапы используют ИИ для управления потоком данных и расстановки приоритетов в режиме реального времени.

Инвесторы обращают внимание на эту тенденцию. По последним прогнозам, к 2028 году рынок искусственного интеллекта для кибербезопасности будет стоить 35,43 миллиарда долларов, что означает среднегодовой темп роста более 23%.

2. Конфиденциальность и соответствие

Правила конфиденциальности являются главным приоритетом в Европе, и США не сильно отстают. В ответ на это ожидается, что рынок конфиденциальности данных увидит значительный среднегодовой темп роста 40,8%, что приведет к 25,85 миллиардам к 2029 году.

Ужесточение законов о конфиденциальности данных открыло двери для стартапов программного обеспечения для обеспечения конфиденциальности данных, чтобы предлагать такие решения, как автоматизация управления конфиденциальностью на основе облачных технологий и мониторинг деловой практики на местах, чтобы убедиться, что они соответствуют рыночным нормам.

3. Безопасность Интернета вещей

Целых 98% данных устройств IoT не зашифрованы, что представляет собой серьезную угрозу безопасности. По мере того, как организации более полно используют IoT, стартапы извлекают из этого выгоду, предлагая решения для защиты от вредоносных программ и атак с целью кражи личных данных.

По оценкам GSMA, к 2025 году количество соединений IoT достигнет 25,2 миллиарда, а к 2028 году рынок безопасности IoT достигнет 61,6 миллиарда долларов.

4. Нулевое доверие

Я думаю, что это, пожалуй, самый многообещающий тренд кибербезопасности. Прежде чем технология достигла своего нынешнего уровня интеграции во все аспекты нашей жизни, компании могли использовать подход к обеспечению безопасности «глубокоэшелонированной защиты». DiD использует уровни контроля безопасности, чтобы установить периметр внутри системы, чтобы обеспечить ее безопасность. Это уже невозможно из-за популярности облачных приложений, работы из дома и других трендов.

В настоящее время компании используют подход «нулевого доверия» для защиты современных цифровых сред. Инвесторы обращают на это внимание и выделяют деньги на модернизацию систем с помощью технологии нулевого доверия. Один из крупнейших чеков был выплачен калифорнийской компании на 300 миллионов долларов. Другие, более мелкие группы внедрили системы безопасности с нулевым доверием, которые требуют подтверждения личности в каждой точке доступа.

Это успешно ограничивает кибератаки со стороны облачных вычислений, доступа к Интернету вещей и глобальных уязвимостей удаленной рабочей силы. Альмог Апирион отмечает, что нулевое доверие продолжит вытеснять VPN, потому что при нулевом доверии идентификация «является новым ключом доступа». (Полное раскрытие: Apirion является генеральным директором компании в моем портфолио.) Это обеспечивает более контролируемый доступ к необходимым ресурсам без раскрытия всех цифровых активов.

Системы с нулевым доверием также могут помочь в решении проблем соответствия, делая их еще более привлекательными для бизнеса и инвесторов. Исследования показывают, что 72% глобальных организаций заинтересованы во внедрении технологии нулевого доверия.

Успех в текущем ландшафте

Пространство кибербезопасности переполнено, поэтому основатели могут столкнуться с неожиданными препятствиями прямо сейчас. Конкурентный характер рынка также означает, что здесь меньше места для ошибок.

В конечном счете, мой лучший совет для основателей на текущем рынке — выделиться, решая существенную проблему интересным и эффективным способом. Это отличный способ привлечь внимание инвесторов, что очень важно на первых этапах.

Поиск инновационных решений в области кибербезопасности может помочь основателям добиться успеха в будущем, потому что это не только заинтересует инвесторов, но и заложит основу для создания крупной и прибыльной компании в долгосрочной перспективе. Интернет, несомненно, останется опорой нашего общества.

Киберпреступность обходится мировой экономике в 2,9 миллиона долларов каждую минуту, и многие предприятия не имеют средств для защиты от этих атак. Это означает, что кибербезопасность также будет играть все более важную роль в

нашей жизни. В то время как инвесторы могут выбирать свои оценки более тщательно, компании с инновационными и эффективными стратегиями все еще могут привлекать значительное венчурное финансирование». ***(Sergey Gribov. Navigating The Cybersecurity Funding Landscape // Forbes (https://www.forbes.com/sites/forbesbusinesscouncil/2022/09/02/navigating-the-cybersecurity-funding-landscape/?sh=1c26463d67f0). 02.09.2022).***

***

«Может ли любая организация избежать риска, когда речь идет о кибербезопасности? Нет. Это плохие новости.

Но может ли каждая организация предпринять шаги для создания и развития сильной культуры безопасности, чтобы минимизировать риски? Да. Это хорошая новость.

Один из важных шагов, который может предпринять каждая организация, — постоянно обсуждать вопросы кибербезопасности, чтобы привлечь к этому внимание всех сотрудников. Но есть правильные — и неправильные — способы обрамления этих разговоров.

Правильный способ: говорить сверху вниз.

Неправильный путь: возложите на ИТ ответственность за коммуникацию в сфере кибербезопасности.

Во многих организациях ИТ-директор или ИТ-отдел считаются «владельцами» сообщения о кибербезопасности. В конце концов, они отвечают за технологию, верно? Возможно. Но за что они не отвечают, так это за людей во всей организации во всех условиях, во всех отделах и на всех ролях.

Эффективные обсуждения кибербезопасности начинаются на самом верху организации — на уровне правления — и просачиваются на все уровни, от высшего руководства до передовых.

…Продвигайте важность включения кибербезопасности в повестку дня каждого заседания совета директоров и убедитесь, что каждый член совета директоров понимает риски и критические элементы ваших мер кибербезопасности — как связанных с технологиями, так и с людьми, — чтобы они могли ходить пешком и говорить.

Правильный путь: сосредоточиться на защите человеческого уровня.

Неправильный путь: сосредоточьтесь на технологических исправлениях.

Многие разговоры о кибербезопасности, которые происходят в организациях, сосредоточены на брандмауэрах, системах обнаружения и предотвращения вторжений, защите конечных точек, безопасных шлюзах электронной почты и других передовых технических решениях.

Это важно, но этого недостаточно.

Современные организации не могут позволить себе пренебрегать средствами защиты на человеческом уровне. Мы знаем, что 85% нарушений безопасности можно отнести к человеческим ошибкам.

Ваши разговоры с вашими сотрудниками должны быть больше сосредоточены на них, а не на ваших технологиях. Это должно помочь им понять критическую роль, которую они могут сыграть как в защите, так и в потенциальной угрозе вашим

данным и системам. Он должен быть разработан, чтобы помочь им понять, как даже очень простые и, казалось бы, безобидные действия, такие как оставить свой компьютер включенным и доступным во время короткого перерыва или открыть подозрительное электронное письмо, могут угрожать вашим усилиям по кибербезопасности.

Правильный способ: рассказывайте истории.

Неправильный путь: сосредоточьтесь на данных и деталях.

Представьте себе типичный разговор о кибербезопасности: кто-то из ИТ-отдела, скорее всего, вытаскивает презентацию и слайд за слайдом просматривает серию диаграмм и графиков, заполненных огромным количеством жаргона и аббревиатур, с которыми даже некоторые сотрудники ИТ-команды не знакомы.

Это не способ привлечь сотрудников и заручиться их поддержкой в ваших усилиях по кибербезопасности.

Вместо этого рассказывайте истории — истории, которые находят отклик у вашей аудитории и убедительно иллюстрируют, как их действия могут помочь или навредить вашим усилиям. Включите истории из СМИ, например; их много, к сожалению. Эти примеры могут передать последствия их потенциальных действий более четко, чем сложенный график.

Расскажите истории о том, как взлом повлиял на сотрудников вашей организации и как они отреагировали. И даже объясните, если эти люди захотят или их личность может быть защищена, как люди в вашей организации были обмануты, чтобы подвергнуть риску системы и данные.

Соответствующие показатели могут быть включены в эти разговоры по мере необходимости. Но поднятие ваших разговоров о безопасности до уровня истории может помочь вам решить, какие метрики поделиться и сколько подробностей вдаваться. Всегда фильтруйте свои разговоры о кибербезопасности через историю.

Правильный путь: рассматривайте свои разговоры как путешествие, а не пункт назначения.

Неправильный путь: проводите беседы во время адаптации и ежегодного обслуживания.

Довольно часто разговоры о кибербезопасности происходят только во время адаптации, в момент найма и ежегодно во время необходимых сессий сотрудников без отрыва от работы.

Этого не достаточно.

С одной стороны, сотрудники по понятным причинам перегружены во время этих событий. Слишком много информации обрушивается на них одновременно, и они не могут знать, на чем сосредоточиться или как расставить приоритеты в сообщениях, которые они получают.

Во-вторых, безопасность должна быть путешествием и разговором — на самом деле, многими разговорами, а не пунктом назначения и директивой.

За последние несколько лет в технологиях, связанных с безопасностью, было достигнуто бесчисленное множество достижений. К сожалению, эти достижения не останавливают волну нарушений. Ни одна организация никогда не застрахована от угроз кибератак. Но вы можете быть лучше подготовлены и защищены, если будете вести правильные разговоры». ***(Perry Carpenter. The Right (And Wrong) Way To***

Frame Cybersecurity Conversations // Forbes (https://www.forbes.com/sites/forbesbusinesscouncil/2022/09/08/the-right-and-wrong-way-to-frame-cybersecurity-conversations/?sh=f8637091d9bf). 08.09.2022).

***

«Когда люди думают о кибербезопасности, они часто думают о технических мерах безопасности, помогающих защитить их бизнес. Хотя эти меры, включая программное обеспечение для защиты конечных точек и брандмауэры, важны, их недостаточно для создания киберустойчивой организации. Поведение сотрудников также имеет решающее значение для киберзащиты организации, поскольку 82% утечек данных в 2021 году были связаны с «человеческим фактором».

Киберугрозы — неотъемлемая часть цифровой эпохи, и кибератаки будут становиться все более изощренными. Лучший способ для организаций защитить себя — создать культуру осведомленности о кибербезопасности и разработать четкие стратегии, гарантирующие, что сотрудники смогут обнаруживать атаки.

При правильном подходе и ИТ-инфраструктуре сотрудники могут стать одним из самых эффективных средств контроля безопасности. Ключом к созданию влиятельной культуры кибербезопасности является признание того, что люди могут представлять собой мощную первую линию защиты от кибератак.

1. Создание культуры начинается сверху.

Хотя культивирование культуры кибербезопасности является сложной задачей, одним из наиболее важных моментов является то, что оно должно начинаться сверху. Чтобы поощрять отношение сотрудников к безопасности, руководители высшего звена должны подавать пример и задавать тон для повышения осведомленности во всей организации. Руководители не могут ожидать, что их сотрудники прислушаются к проблемам кибербезопасности, если это не является ключевым приоритетом для управленческой команды.

Руководители также должны активно продвигать ключевые сообщения для сотрудников на корпоративных мероприятиях, как виртуально, так и лично. Например, вы можете начинать каждое общее собрание сотрудников с рассказа о кибербезопасности, чтобы показать всем в вашей организации, что это неотъемлемая часть корпоративных ценностей.

Информация о кибербезопасности должна предоставляться четко, чтобы сотрудники компании понимали важность безопасного поведения в Интернете. Если вы хотите способствовать изменениям, важно общаться в терминах, понятных сотрудникам, чтобы цели были ясно поняты. Обмен сообщениями имеет решающее значение для вовлечения и развития культуры кибербезопасности.

2. Создайте программы повышения осведомленности о безопасности, адаптированные для различных групп.

Поскольку киберугрозы с каждым днем становятся все более сложными, организации должны следить за тем, чтобы команды постоянно обучались кибербезопасности, чтобы оставаться защищенными. Чтобы держать сотрудников в курсе последних угроз, директора по информационной безопасности (CISO) могут сотрудничать с отделом кадров (который обычно руководит корпоративными

программами обучения) для организации программ повышения осведомленности о безопасности.

При планировании этих программ предприятия также должны помнить, что вовлеченность сотрудников является ключом к участию. Это означает, что простого создания слайд-шоу будет недостаточно. Вместо этого сотрудники должны быть непосредственно вовлечены в свое обучение. Один из способов поощрения участия сотрудников состоит в том, чтобы включать стимулы, ставить командные цели и вознаграждать их при достижении целей.

С другой стороны, в то время как программы повышения осведомленности о безопасности обычно в значительной степени сосредоточены на сотрудниках, рост компрометации деловой электронной почты и атак социальной инженерии подтверждает, что руководители также нуждаются в регулярном обучении. Топ-менеджеры и члены правления — это особые группы, которым требуется специальное обучение для удовлетворения их уникальных потребностей. Эти программы должны включать типы атак, нацеленных на руководителей, чтобы научить их защищаться от уязвимостей в этих областях.

3. Одного общения недостаточно.

Даже если у вас есть надлежащая программа повышения осведомленности о кибербезопасности, рассмотрите возможность имитации атак социальной инженерии, которые имитируют реальные фишинговые атаки, поскольку такие тренировки могут помочь сотрудникам сохранять бдительность.

Организации также должны поощрять сотрудников быть более активными при столкновении с чем-либо, что может увеличить риск утечки данных. Например, сотрудники должны напоминать друг другу, что нельзя оставлять свои корпоративные устройства без присмотра, особенно если они еще не вошли в систему, чтобы предотвратить несанкционированный доступ.

Защитите свой бизнес с вашими людьми.

Осведомленность о кибербезопасности должна быть жизненно важна для каждого бизнеса для защиты от киберрисков. Организации должны помнить, что культура также может использоваться в качестве тактики и инструмента кибербезопасности; его необходимо постоянно оценивать, укреплять и адаптировать. В конечном счете, цель любой организации должна состоять в том, чтобы развивать культуру кибербезопасности, чтобы обеспечить организационную устойчивость и свести к минимуму потери при столкновении с кибератакой». ***(Parvinder Walia. Building A Cybersecurity Culture In Your Organization // Forbes (https://www.forbes.com/sites/forbestechcouncil/2022/09/13/building-a-cybersecurity-culture-in-your-organization/?sh=19360ceb47a9). 13.09.2022).***

***

«Науковці канадської університетської лабораторії Гуельфа, яка займається кіберзагрозами в сільському господарстві, попередили про дуже низький рівень кібербезпеки у світовому сільському господарстві.

У найновішому звіті працівників лабораторії, опублікованому у науковому журналі Applied Sciences, зазначено, що рівень кібербезпеки в сільському господарстві мінімальний або взагалі відсутній. При цьому сектор дедалі активніше

використовує ІТ-обладнання, сенсорні мережі та комп'ютерну техніку. Така ситуація, на думку науковців, робить галузь особливо вразливою.

У звіті наголосили, що серед найпоширеніших загроз — блокування комп'ютерної системи фермера та викрадення даних. У першому випадку часто хакери вимагають викуп за розблокування. У другому — може йтися про різні дані, навіть незначні на перший погляд. Наприклад, температуру у теплиці чи інформацію про час годування тварин. Однак таке втручання може призвести до збоїв у роботі господарства з серйозними наслідками.

— Будь-який збій в інфраструктурі може порушити мережу поставок і вплинути на продовольчу безпеку, — пояснив керівник лабораторії д-р Алі Дегантанха, звернувши увагу на поточну ситуацію в Україні.

Окрім цього науковці відмітили інший тип загрози, який зараз активно зростає — від «підтримуваних іноземними урядами хакерів, метою яких є зрив роботи чи отримання контролю над мережами». Фахівці виявили такі кіберзагрози для сільського господарства переважно з боку Китаю, росії, Північної Кореї та Ірану.

Вчені наголосили, що аграрії у всьому світі повинні більше уваги приділяти цифровій безпеці та захисту даних. Особливо у сучасних умовах загроз продовольчій безпеці». ***(Науковці виявили ряд кіберзагроз для світового агросектора, контрольованих урядами росії, Китаю, Північної Кореї та Ірану // Growhow.in.ua (https://www.growhow.in.ua/naukovtsi-vyiavyly-riad-kiberzahroz-dlia-svitovoho-ahrosektora-kontrolovanykh-uriadamy-rosii-kytaiu-pivnichnoi-korei-ta-iranu/). 14.09.2022).***

***

«…Есть несколько вещей, которые вы должны учитывать при выборе директора по информационной безопасности для своего стартапа. Во-первых, человек должен иметь опыт управления значительными киберугрозами и инцидентами. Во-вторых, они должны быть в состоянии сформулировать приоритеты кибербезопасности для высшего руководства и объяснить, какую пользу их инициативы принесут бизнесу. Наконец, директор по информационной безопасности должен иметь возможность эффективно общаться с заинтересованными сторонами — внутренними и внешними — для поддержания согласованной стратегии между отделами.

При выборе директора по информационной безопасности для вашего стартапа важно учитывать ряд факторов, в том числе размер компании, отрасль и профиль рисков. Вот несколько основных критериев выбора:

Размер: стартапу с менее чем 50 сотрудниками может не понадобиться штатный директор по информационной безопасности, в то время как компании с более чем 200 сотрудниками, скорее всего, понадобится.

Отрасль: директоров по информационной безопасности следует выбирать на основе типа рисков информационной безопасности, которые преобладают в их соответствующих отраслях.

Профиль риска стартапа: стартапу с продуктами или услугами с высоким риском может потребоваться более опытный директор по информационной безопасности, чем компании с продуктами или услугами с меньшим риском.

Профиль риска компании также может повлиять на тип опыта и образования, необходимых для должности.

Тип должности: стартапу может потребоваться временный или постоянный директор по информационной безопасности, в зависимости от стадии его развития и уровня риска, связанного с его данными и операциями.

Прежде чем выбрать директора по информационной безопасности, вы должны иметь четкое представление об обязанностях директора по информационной безопасности и его миссии в вашем стартапе. Директор по информационной безопасности отвечает за надзор за общей стратегией безопасности и операциями компании. Эта должность обычно подчиняется генеральному директору или главному операционному директору. Ниже приведены некоторые из обязанностей CISO:

Руководство общей стратегией кибербезопасности и операциями

Направление и управление программой управления киберрисками

Управление управлением информационной безопасностью и соответствием требованиям

Управление процессами оценки и управления информационными рисками

Обеспечение лидерства в разработке планов реагирования на инциденты и управление группами реагирования на инциденты

Развитие прочных партнерских отношений с внешними организациями, такими как правоохранительные органы, SOC и поставщики данных.

…ключевые факторы, которые следует учитывать при выборе директора по информационной безопасности для вашего стартапа, включают:

1. Лидерство и управленческий опыт. Хороший директор по информационной безопасности должен иметь большой опыт в области лидерства и управления, что поможет ему задавать направление и эффективно управлять ресурсами команды.

2. Экспертиза в области безопасности. Хороший директор по информационной безопасности должен хорошо разбираться в технологиях безопасности и уметь разрабатывать инновационные решения для защиты данных и активов компании.

3. Деловая хватка. Хороший директор по информационной безопасности должен понимать бизнес-цели компании и то, как безопасность влияет на эти цели.

4. Стратегическое мышление. Хороший директор по информационной безопасности должен уметь стратегически мыслить о проблемах безопасности и разрабатывать долгосрочные планы по их решению.

5. Навыки межличностного общения. Хороший директор по информационной безопасности должен обладать сильными навыками межличностного общения, которые помогут ему строить отношения с высшим руководством внутри компании и эффективно общаться с общественностью.

…четыре совета по построению отношений с вашим директором по информационной безопасности:

1. С самого начала установите четкие ожидания: убедитесь, что вы знаете, за что отвечает ваш директор по информационной безопасности и каковы его ограничения. Установление четких границ поможет гарантировать, что обе стороны работают для достижения одних и тех же целей.

2. Будьте откровенны со своим директором по информационной безопасности: делитесь всеми необходимыми данными и информацией, как только они становятся доступными. Это поможет им быть в курсе вашего бизнеса и наоборот.

3. Поддерживайте открытое общение: регулярное общение поможет укрепить доверие между вами и вашим директором по информационной безопасности и обеспечит обе стороны самой последней информацией о прогрессе вашей компании.

4. Создавайте атмосферу сотрудничества: работайте вместе над поиском решений общих проблем и поощряйте взаимное уважение и сотрудничество между членами команды.

Одна из самых важных и деликатных ролей, которую может назначить организация, — это директор по информационной безопасности. Этот человек должен быть в состоянии сбалансировать безопасность с инновациями, и он должен иметь глубокое понимание технологий, чтобы принимать обоснованные решения о том, как лучше всего защитить данные своей компании. Прежде всего, вам нужен человек, хорошо разбирающийся в кибербезопасности и имеющий опыт руководства командой экспертов. Во-вторых, убедитесь, что выбранный вами директор по информационной безопасности обладает полномочиями и ресурсами, необходимыми для борьбы с любыми потенциальными киберугрозами, с которыми сталкивается ваша компания. И, наконец, обязательно учитывайте биографию и опыт кандидата при оценке его пригодности для этой роли. Выполняя эти шаги, вы можете гарантировать, что ваш стартап имеет наилучшие шансы защитить себя от онлайн-угроз». ***(Jim Koohyar Biniyaz. What to Look for When Hiring a CISO for a Growing Startup // Entrepreneur Media, Inc. (https://www.entrepreneur.com/growing-a-business/what-to-look-for-when-hiring-a-ciso-for-a-growing-startup/433828). 16.09.2022).***

***

«Спрос на специалистов по кибербезопасности резко вырос за последнее десятилетие из-за роста числа киберпреступлений. В результате карьера в области кибербезопасности приносит многочисленные преимущества, в том числе безопасность работы и относительно высокий доход.

В этой статье мы расскажем о средней зарплате в области кибербезопасности, включая разницу в доходах в зависимости от должности и штата.

Средняя зарплата в сфере кибербезопасности

Бюро статистики труда США (BLS) сообщает, что средняя годовая зарплата аналитиков по информационной безопасности составляет 102 600 долларов. Эта зарплата более чем вдвое превышает средний национальный заработок работников во всех отраслях (45 760 долларов США).

Потенциал заработной платы в области кибербезопасности, как правило, настолько высок из-за деликатного характера работы и растущего экономического спроса на специалистов по кибербезопасности.

Заработная плата по отраслям

Преимущество работы специалистом по кибербезопасности в том, что он может выбирать из множества отраслей. Как специалист по кибербезопасности,

конкретная отрасль, в которой вы работаете, играет важную роль в определении вашего годового дохода.

Давайте посмотрим на некоторые высокооплачиваемые отрасли, где, по данным BLS, востребованы специалисты в области кибербезопасности.

Рекультивация и другие услуги по обращению с отходами. Аналитики по информационной безопасности в этом секторе получают среднюю годовую заработную плату в размере 173 250 долларов США.

Другие информационные услуги. Этот ИТ-подсектор платит экспертам по кибербезопасности в среднем 149 540 долларов.

Производство компьютерной и периферийной техники. Специалисты по кибербезопасности в этой области зарабатывают в среднем 144 040 долларов.

Ценные бумаги и другие финансовые инвестиционные сектора. В этих областях средняя зарплата в области кибербезопасности составляет 142 070 долларов.

Киноиндустрия и видеоиндустрия. Этот подсектор развлечений платит аналитикам по информационной безопасности среднюю годовую заработную плату в размере 141 070 долларов.

Зарплата по штату

Помимо отрасли, географическое положение является важным фактором, определяющим заработную плату в сфере кибербезопасности. Заработная плата различается в зависимости от штата, потому что работодатели часто используют ставку подоходного налога и прожиточный минимум своего штата для определения заработной платы.

Вполне логично, что самые высокие зарплаты в области кибербезопасности выплачиваются в мегаполисах с относительно высокой стоимостью жизни. Ознакомьтесь со списком ниже, чтобы увидеть штаты, в которых профессионалы могут получать высокие средние зарплаты в области кибербезопасности, согласно BLS.

Калифорния: 135 200 долларов.

Нью-Йорк: 133 210 долларов.

Мэриленд: 126 110 долларов

Айова: 125 650 долларов.

Округ Колумбия: 124 980 долларов.

Заработная плата в сфере кибербезопасности по должностям

Заработная плата в области кибербезопасности также может варьироваться в зависимости от уровня опыта и должности. Однако в целом потенциал заработка в этой отрасли настолько высок, что даже специалист по кибербезопасности начального уровня может получить шестизначный доход.

По состоянию на август 2022 года Cyberseek перечисляет приведенные ниже цифры как средний уровень доходов специалистов по кибербезопасности на различных должностях.

Роли начального уровня

Новички в этой отрасли обычно проводят от трех до пяти лет на начальных должностях в области кибербезопасности, чтобы приобрести базовый опыт. Из

приведенных ниже рисунков вы увидите, что должность начального уровня в области кибербезопасности не означает низкую оплату.

Специалист по кибербезопасности

Средняя годовая зарплата: 104 480 долларов США.

Вакансий: 11 150

Краткое описание должности: Специалист по кибербезопасности ищет сетевые и системные угрозы посредством регулярного сканирования уязвимостей. Они разрабатывают стратегии безопасности, направленные на защиту целостности данных их компании.

Аналитик по киберпреступности

Средняя годовая зарплата: 100 000 долларов США.

Вакансий: 1388

Краткое описание должности: Этот профессионал расследует атаки вредоносных программ, людей, стоящих за ними, и причиненный ущерб. Аналитик киберпреступности также работает над восстановлением конфиденциальных данных, которые могут быть полезны для судебного дела.

Аналитик инцидентов и вторжений

Средняя годовая зарплата: 88 230 долларов США.

Вакансий: 11 169

Краткое описание позиции: Аналитик инцидентов и вторжений обнаруживает угрозы безопасности в сети организации. Они также предотвращают эскалацию этих угроз и сообщают о своих выводах старшим экспертам по кибербезопасности.

ИТ-аудитор

Средняя годовая зарплата: 110 000 долларов США.

Вакансий: 9 639

Краткое описание должности: Эта роль начального уровня включает постоянную оценку ИТ-инфраструктуры компании для обеспечения всесторонней безопасности и соблюдения нормативных требований.

Роли среднего уровня

Получив не менее пяти лет опыта работы на начальных должностях, специалисты по кибербезопасности могут продвигаться по карьерной лестнице. Должности среднего уровня означают большую ответственность и более высокую зарплату в сфере кибербезопасности.

Давайте посмотрим на некоторые из них ниже.

Аналитик по кибербезопасности

Средняя годовая зарплата: 107 500 долларов США.

Вакансий: 39 629

Краткое описание должности: эта должность включает анализ кибератак, вредоносного ПО и поведения киберпреступников. После анализа аналитик по кибербезопасности разрабатывает меры безопасности для предотвращения повторения таких атак.

Консультант по кибербезопасности

Средняя годовая зарплата: 92 500 долларов США.

Вакансий: 27 226

Краткое описание должности: Консультант по кибербезопасности тестирует сетевую безопасность организации, обнаруживает уязвимости и разрабатывает лучшую систему безопасности.

Тестер проникновения и уязвимостей

Средняя годовая зарплата: 101 090 долларов США.

Вакансий: 34 505

Краткое изложение позиции: Эта должность посвящена этичному взлому. Тестер проникновения и уязвимости имитирует реальные кибератаки на существующие системы, чтобы обнаруживать бреши в системах безопасности до того, как злоумышленники смогут взломать их.

Расширенные роли

Продвинутые роли зарезервированы для опытных специалистов с 10-15-летним опытом работы в области кибербезопасности. Эксперты по кибербезопасности на руководящих должностях обычно руководят аналитиками среднего и младшего звена.

Менеджер по кибербезопасности

Средняя годовая зарплата: 130 000 долларов США.

Вакансий: 27 633

Краткое описание должности: Эта управленческая должность предполагает делегирование определенных обязанностей младшим специалистам по кибербезопасности. Менеджер по кибербезопасности также создает стратегии для предотвращения нарушений безопасности.

Инженер по кибербезопасности

Средняя годовая зарплата: 117 510 долларов США.

Вакансий: 78 288

Краткое описание должности: Этот специалист по кибербезопасности разрабатывает высокотехнологичные решения для защиты цифровых активов компании от программ-вымогателей, хакеров и внутренних угроз.

Архитектор кибербезопасности

Средняя годовая зарплата: 159 750 долларов США.

Вакансий: 9 050

Краткое описание должности: Архитектор кибербезопасности проектирует, создает и внедряет системы безопасности корпоративного класса. Они также помогают другим членам группы кибербезопасности эффективно внедрять протоколы безопасности.

Перспективы работы в области кибербезопасности

В 2016 году уровень безработицы в сфере кибербезопасности упал до 0% и с тех пор остается на этом уровне. Разрыв в талантах продолжает увеличиваться и сегодня. Cybercrime Magazine прогнозирует, что к 2025 году в сфере кибербезопасности появится 3,5 миллиона вакансий.

Индустрия кибербезопасности обеспечивает большую безопасность работы, чем многие другие профессии. Например, по данным BLS, рабочие места для аналитиков по информационной безопасности вырастут на 33% с 2020 по 2030 год. Этот показатель в четыре раза превышает средний темп роста занятости по всем профессиям по стране». ***(Nneoma Uche, Brenna Swanston. What Is A Typical***

Cybersecurity Salary? // Forbes Media LLC. (https://www.forbes.com/advisor/education/cyber-security-salary-outlook/). 07.09.2022).

***

«Компания Google завершила сделку по приобретению компании Mandiant, занимающейся кибербезопасностью, за 5,4 миллиарда долларов, чтобы повысить безопасность своих облачных сервисов.

«Объединение существующего портфолио средств безопасности Google Cloud с ведущими аналитическими данными Mandiant о киберугрозах позволит нам предоставить пакет операций по обеспечению безопасности, который поможет предприятиям во всем мире оставаться защищенными на каждом этапе жизненного цикла безопасности», — написал генеральный директор Google Cloud Томас Куриан в сообщении в блоге компании от 12 сентября..

Google Cloud добавляет в Mandiant функции анализа угроз, управления поверхностью атаки и проверки безопасности. Google предоставляет облачные услуги различным системам здравоохранения.

«Благодаря масштабу обработки данных Google, новым подходам к аналитике с использованием [искусственного интеллекта] и машинного обучения, а также сосредоточению внимания на устранении целых классов угроз, Google Cloud и Mandiant помогут организациям переосмыслить безопасность, чтобы соответствовать требованиям нашего быстро меняющегося мира. — написал г-н Куриан». ***(Giles Bruce. Google completes $5.4B acquisition of cybersecurity firm Mandiant to bolster cloud // Becker's Healthcare (https://www.beckershospitalreview.com/healthcare-information-technology/google-completes-5-4b-acquisition-of-cybersecurity-firm-mandiant-to-bolster-cloud.html). 20.09.2022).***

***

«Lloyd's of London Ltd. сообщила своей глобальной сети страховых групп, что новые или обновленные полисы покрытия киберстрахования должны исключать атаки со стороны государства с 31 марта 2023 года. В качестве причины изменения страховщик назвал системный риск для страхового рынка. также добавляя, что политика также должна исключать потери от войны, если нет отдельного исключения такого типа.

Изменение политики снова поднимает вопросы о том, как классифицируются атаки со стороны государства в целях страхования; очень редко публике доступны четкие доказательства, демонстрирующие, что группа, поддерживаемая государством, несет ответственность за инцидент, при этом мировые правительства приписывают различные действия, начиная от выводов и заканчивая секретной непубличной информацией и простым политическим маневрированием.

«Катастрофические» атаки на национальные государства больше не покрываются андеррайтерами Ллойда с 2023 года.

Фирмы ищут способы сократить покрытие киберстрахования по мере роста расходов, вызванного недавним ростом преступности (особенно программ-

вымогателей). Атаки на национальные государства чаще всего являются целенаправленными и больше связаны со шпионажем, чем с кражей или нанесением ущерба, но последствия иногда распространяются и наносят значительный ущерб другим организациям.

Инцидент с NotPetya в 2017 году, по-видимому, стал основным фактором, повлиявшим на это решение. Затянувшаяся судебная тяжба между Merck и ее флотом страховщиков, причинивших ущерб на сумму более 1,4 миллиарда долларов в результате этой атаки, наконец, закончилась решением в пользу Merck прошедший год. Киберстрахование ранее полагалось на исключение «военных действий» для рассмотрения подобных инцидентов, но постановление создает юридический прецедент, который подрывает эту позицию. Вторжение в Украину вызвало опасения, что подобные киберобмены могут нарушить условия сдерживания и причинить такой же огромный ущерб, особенно критически важной инфраструктуре. Уже был по крайней мере один небольшой инцидент такого рода — вредоносное ПО AcidRain, которое было нацелено на украинский сервис ViaSat в начале войны, но также оказалось в крупной ветряной установке в Германии.

Страховщики стремятся снизить риск, поскольку компании увеличивают спрос на покрытие киберстрахования, и такое колебание динамики рынка вызывает серьезную реорганизацию отрасли. Lloyd's уже некоторое время планировал изменение такого рода, разработав в конце 2021 года ряд новых договорных положений, которые были направлены на уточнение того, когда кибератаки можно считать актами войны и наносить достаточно катастрофический ущерб, чтобы исключить их из охвата.

В условиях освобождения от нового соглашения Ллойда указаны несколько конкретных стран: Китай, Франция, Япония, Россия, Великобритания и США. В нем также называются конкретные основные услуги, которые могут быть освобождены от покрытия киберстрахования, если национальные атаки наносят им вред: среди них финансовые учреждения, инфраструктура финансового рынка, медицинские и коммунальные услуги. У управляющих агентов есть некоторая свобода действий, чтобы включить свои собственные пункты, но они должны сначала объяснить свой подход и получить разрешение от Lloyd's.

Условия покрытия киберстрахования позволяют страховщику делать «умозаключения» без указания государства

Все предстоящие изменения в покрытии киберстрахования зависят от того, как определяются атаки национального государства. Это, пожалуй, самая спорная часть аранжировки. Lloyd's будет полагаться на атрибуцию правительства, но это не единственный квалификатор. При отсутствии такой атрибуции компания оставляет за собой право самостоятельно сделать «объективно разумный вывод». Он намерен принять эти решения, если правительство потратит «неразумное количество времени, не сделает или не сможет приписать кибероперацию другому государству или тем, кто действует от его имени».

Формулировка «действовать от своего имени» создает особую путаницу в отношении определенных типов атак, не связанных с национальным государством. За атаками программ-вымогателей часто стоят российские хакерские группы, на которые государство долгое время закрывает глаза, но не обязательно связано с ними

или оказывает им какую-либо материальную поддержку. Похоже, что формулировка включена специально для того, чтобы связать такого рода независимые преступные группы с нападениями на национальные государства.

По некоторым прогнозам, всего за год количество организаций, которые не могут позволить себе адекватное покрытие киберстрахования, удвоится. Сейчас, когда средний размер требований о выкупе достигает нескольких миллионов долларов, а затраты на очистку часто исчисляются десятками миллионов, многие компании полностью рассчитывают на страховку для покрытия платежей, когда на них обрушиваются атаки программ-вымогателей.

Общее ужесточение рынка киберстрахования из-за увеличения затрат началось более года назад, когда AXA France стала первой из крупных страховых компаний, которая урезала возмещение платежей от программ-вымогателей из своих предложений. К концу 2021 года наметилась установившаяся тенденция изменения страховщиками цен, лимитов и покрытия; к концу года на рынке произошло довольно стандартное сокращение лимитов вдвое.

Дэвид Линднер, директор по информационным технологиям компании Contrast Security, рассматривает это изменение рынка как «новую норму» и побуждение организаций обеспечить их надлежащую защиту в максимально возможной степени: «Организации не могут просто полагаться на свой полис киберстрахования и должны заранее защитить себя от этих катастрофических кибератак». ***(Scott Ikeda. Lloyd's of London: Nation-State Attacks No Longer a Part of Cyber Insurance Coverage as of 2023 // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/lloyds-of-london-nation-state-attacks-no-longer-a-part-of-cyber-insurance-coverage-as-of-2023/). 06.09.2022).***

***

«Стоимость и условия киберстрахования были проблемой для предприятий всех типов с 2021 года, когда стремительный рост стоимости платежей и исправлений программ-вымогателей заставил страховые компании пересмотреть свои варианты. Новое исследование от BlackBerry и Corvus Insurance показывает, что этот новый ландшафт вызывает хроническую нехватку киберпокрытия для бизнеса.

Дефицит киберстрахования: 80% предприятий не будут иметь достаточного покрытия для текущего среднего спроса на программы-вымогатели

В опросе приняли участие 450 лиц, принимающих решения в области ИТ и кибербезопасности в компаниях, расположенных в США и Канаде. В настоящее время организациям в этой части мира приходится платить в среднем миллионы долларов, а средняя стоимость расследования и восстановления составляет 2,4 миллиона долларов.

Однако только 55% опрошенных организаций вообще застрахованы от киберугроз. И из тех, кто застрахован, чуть менее 20% имеют покрытие более 600 000 долларов; недостаточно, чтобы покрыть обычную плату за вымогателей, не говоря уже о потенциальных затратах на очистку.

Особые трудности испытывает малый и средний бизнес. У них часто просто не хватает средств для покрытия страховых взносов, и они могут столкнуться с

потенциальным разорением в случае кибератаки. Только 14% малых предприятий со штатом менее 1500 сотрудников имеют покрытие киберстрахования на сумму 600 000 долларов и более. Кроме того, 37% застрахованных не покрывают платежи от программ-вымогателей, а 43% не покрывают дополнительные расходы на восстановление, такие как время простоя и судебные издержки.

Несмотря на то, что большинству предприятий не хватает надлежащего покрытия, они, тем не менее, говорят, что ищут своих партнеров для обеспечения адекватной киберстраховки. 60 % респондентов заявили, что пересмотрят деловые партнерские отношения, если партнер не будет иметь «комплексного» покрытия киберстрахования, а 68 % ИТ-специалистов заявили, что пересмотрят эти отношения, если методы партнерской кибербезопасности (например, внедрение технологий) будут отсутствует.

В исследовании отмечается, что в дополнение к общему увеличению стоимости и ужесточению условий и покрываемых событий компании по киберстрахованию также все чаще просят клиентов продемонстрировать ключевые контрольные показатели безопасности, когда они приходят на борт или продлевают полисы. Это еще одна область, в которой малый бизнес может столкнуться с трудностями из-за нехватки бюджета или отсутствия готовности. Некоторые компании не понимают, что страховщики в первую очередь хотят видеть хорошо реализованное программное обеспечение для обнаружения и реагирования на конечных точках (EDR), о чем они могут не узнать, пока не получат письмо, объясняющее, почему запрос на покрытие был отклонен. 34% опрошенных получили отказ именно по этой причине.

Шон Сербер, вице-президент по архитектуре и стратегии решений Tanium, задается вопросом, насколько полезно внедрение программного обеспечения EDR при определении такого рода киберстрахования: «Затраты значительно различаются, и их трудно спрогнозировать не из-за зрелости программы кибербезопасности, а вместо этого зависит от того, насколько зрелы их операционное аварийное восстановление и планы обеспечения непрерывности бизнеса. Такие решения, как EDR, могут привести к ложному чувству безопасности, поскольку после обнаружения угрозы может быть уже слишком поздно. Это означает, что организациям необходимо сосредоточиться на обеспечении видимости и контроля над своей средой до атаки программ-вымогателей, а не после нее. Это требует тесной интеграции между группами эксплуатации и безопасности, а также консолидации их инструментов, чтобы они работали с одним и тем же источником достоверной информации, фактическим состоянием конечных точек и устройств в своей сети.

«В конечном счете, киберстрахование может потребовать от компании пройти «физическую» проверку, как если бы кто-то сделал это для полиса страхования жизни, чтобы проверить текущее состояние своей кибербезопасности и соответствующую страховку, необходимую для защиты их интересов. Идеальным сценарием для киберстраховщиков была бы возможность активно опрашивать сети своих клиентов, чтобы определять уязвимости по мере обнаружения новых угроз, чтобы обеспечить постоянную защиту своей среды».

Организации, надеющиеся на помощь правительства в выплатах программ-вымогателей, могут столкнуться с неприятным пробуждением

Все это происходит на фоне индустрии программ-вымогателей, которая в последние годы росла со скоростью лесного пожара и, по прогнозам, продолжит расти в ближайшем будущем. Когда одна крупная банда вымогателей уничтожается, на смену ей приходит одна или несколько (и часто добавляют новые «функции» для загрузки).

Если организации не могут или не будут иметь киберстрахование, которое покрывает реалистичные ожидаемые расходы, как они планируют действовать в случае неожиданного платежа от программы-вымогателя? Большинство (59%) говорят, что ожидают, что правительство выручит их, по крайней мере, если нападение может быть связано с национальным государством. В августе правительство развернуло веб-сайт «StopRansomware.gov», чтобы централизовать ресурсы для восстановления и ускорить оказание кризисной помощи организациям, но средства на помощь в восстановлении ограничены и зависят от квалификационных критериев.

Результаты опроса появились после того, как лондонская компания Lloyd's недавно объявила, что их сеть страховщиков больше не будет покрывать ущерб, причиненный хакерскими атаками на уровне государства, хотя они далеко не единственный вариант на рынке, эта тенденция может распространиться на других страховщиков (особенно если она выдержит неизбежные судебные разбирательства).

Это оставляет недостаточно застрахованные организации просто надеяться, что правительство увеличит свою помощь жертвам программ-вымогателей, что в лучшем случае шаткое положение, учитывая экономические и бюджетные реалии и вероятность того, что большее количество жертв будет нуждаться в постоянно растущем объеме помощи. Гэри Дэвис, старший директор по кибербезопасности BlackBerry, выразил серьезную озабоченность по поводу количества организаций, которые полагаются на государственную помощь; BlackBerry предлагает фирмам с проблемами ИТ-бюджета обратиться к поставщику управляемых услуг кибербезопасности (MSP), который, по крайней мере, соответствует минимальным стандартам, требуемым полисами киберстрахования. Поставщики страховых услуг также могут существенно снизить ставки, если организации захотят поделиться информацией о состоянии безопасности, что-то вроде скидок на автострахование, предлагаемых за установку устройства мониторинга.

Джон Ганн, генеральный директор Token, считает крайне важным, чтобы организации имели адекватную киберстраховку, даже если ее трудно внедрить: «В отчете подчеркивается тот факт, что «страусиный подход» больше нежизнеспособен в эпоху гиперактивности. агрессивные атаки программ-вымогателей. Каждая организация, особенно малый и средний бизнес, ежедневно подвергается все большему риску. Поскольку большинство атак начинаются со скомпрометированных учетных данных пользователя, страховка — лучший способ начать создание надлежащей защиты». ***(Scott Ikeda. "Cyber Insurance Gap" Growing as 80% Of Business Coverage Below Median Ransomware Payment Demand // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/cyber-insurance-gap-growing-as-80-of-business-coverage-below-median-ransomware-payment-demand/). 07.09.2022).***

***

«Женщины составляют 51% населения, но всего 24% специалистов по кибербезопасности. Хорошая новость заключается в том, что организации по кибербезопасности во всем мире все больше признают важность гендерного разнообразия на рабочем месте. Плохая новость заключается в том, что большинство из них по-прежнему борются с наймом и наймом женщин: согласно Глобальному отчету о пробелах в навыках кибербезопасности за 2022 год, семь из 10 руководителей во всем мире считают наем женщин одной из трех своих главных проблем.

Согласно исследованию ISC(2) Cybersecurity Workforce Study, только в Соединенных Штатах насчитывается около 377 000 вакансий, и в 2022 году штат сотрудников должен вырасти на 65%, чтобы эффективно защищать критически важные активы организаций. Тем не менее, что-то должно измениться в найме женщин, чтобы увеличить представительство с 24% от общего числа сотрудников, занимающихся кибербезопасностью, до половины этой рабочей силы.

В то время как разнообразие и инклюзивность стали горячими темами среди руководителей компаний, 70% опрошенных руководителей изо всех сил пытаются нанять не только женщин, но и новых выпускников и представители меньшинств. Но за последние три года, либо из-за этих проблем, либо вопреки им, три из четырех организаций разработали официальные стратегии по найму большего числа женщин, а девять из 10 активно привлекали женщин и новых выпускников. И еще несколько хороших новостей: после пандемии 24% организаций сообщили, что им стало легче нанимать женщин.

При наличии почти 2,5 миллионов рабочих мест в области кибербезопасности 377 000 из этих вакансий расположены в Соединенных Штатах, и эти вакансии увеличивают нагрузку на группы безопасности и организации любого размера. Этот дефицит можно значительно уменьшить, намеренно расширяя набор и наставничество недопредставленных групп, которым есть что предложить.

Женщины привносят разные точки зрения и опыт в сферу кибербезопасности. Это может помочь в борьбе с различными киберпреступниками. Как показало исследование Cloverpop, команды с точки зрения как мужчин, так и женщин принимают лучшие бизнес-решения в 73% случаев.

Что способствует инновациям больше, чем сочетание свежих взглядов, концепций и опыта для решения современных проблем? Поскольку стратегии киберпреступности постоянно меняются, кибербезопасность зависит от такого рода инноваций.

Возможности изобилуют

В качестве первого шага, направленного на преодоление дефицита навыков, организации должны предоставить всем своим сотрудникам, как техническим, так и нетехническим, обучение по вопросам кибербезопасности, чтобы они могли развивать важные навыки кибергигиены. Это включает в себя обучение новейшим методам фишинга и социальной инженерии, а также протоколам надежных паролей.

Для женщины в области кибербезопасности есть множество возможностей и множество возможностей для инноваций. Область предлагает возможности для

роста, захватывающие повседневные задачи и возможность оказать реальное влияние на отдельных лиц, корпорации и национальную безопасность. Существует острая потребность как в женщинах, так и в мужчинах, обладающих навыками и пониманием, необходимыми для борьбы с кибератаками. Это прекрасное время для женщин, чтобы развить свои навыки, чтобы использовать возможности в области кибербезопасности и принять участие в создании более безопасной киберсреды.

Сегодня кибербезопасность является одним из самых быстрорастущих секторов ИТ и одной из самых популярных областей для изучения. Кибербезопасность нужна каждому сектору, включая государственные услуги, здравоохранение, финансы, розничную торговлю и транспорт. Это дает женщинам возможность работать с различными предприятиями и погрузиться в различные отрасли.

Развенчание мифов о кибербезопасности

Существуют также мифы, которые необходимо преодолеть, например идея о том, что кибербезопасность — это мужская работа, а не женская. На самом деле иронично, что мир компьютеров на протяжении десятилетий считался мужской работой, поскольку женщины были первыми, кто создал компьютерный код на перфокартах. Не говоря уже о том, что Ада Лавлейс считается первым в мире программистом, а Маргарет Гамильтон написала программное обеспечение для полетов «Аполлона».

Это приводит к еще одному мифу — убеждению, что вам нужно знать, как программировать, чтобы преуспеть в кибербезопасности. В этой области существует широкий спектр рабочих мест, которые подходят для разных типов личности, навыков и баз знаний, таких как исследования и разработки. И успех в кибербезопасности также требует навыков межличностного общения, таких как соблюдение сроков, принятие на себя ответственности за проекты и задачи, повышение вашей способности решать проблемы и готовность к изменениям по мере развития ситуации.

Возможность для женщин

На сегодняшний день женщины занимают только четверть должностей в области кибербезопасности, необходимых миру для защиты своих критически важных цифровых активов. Тем не менее, кибербезопасность предлагает множество карьерных возможностей и возможностей для женщин. Поскольку технологии и сопутствующие им киберугрозы продолжают развиваться и ускоряться, кибербезопасность также должна развиваться, превращая ее в интеллектуально стимулирующую область для работы.

Разнообразие само по себе не является единственной целью найма женщин на должности в сфере кибербезопасности. Поскольку во всем мире сохраняется разрыв в навыках, это увеличивает риск безопасности для организаций: активное вовлечение женщин в эти роли имеет решающее значение для поддержания цифрового ландшафта и самого нашего образа жизни. В то же время эти вакансии открывают новые возможности и высокий потенциал заработной платы для женщин. Сделать женщин приоритетом при найме на работу — беспроигрышный сценарий для сектора кибербезопасности». ***(Sandra Wheatley. Hiring More Women in Cybersecurity is Mission-Critical // Techstrong Group Inc.***

(https://securityboulevard.com/2022/09/hiring-more-women-in-cybersecurity-is-mission-critical/). 02.09.2022).

***

«…В любой отрасли работа в другой стране несет в себе уникальное понимание. Помимо различных культур на рабочем месте, специалисты по кибербезопасности должны быть готовы столкнуться с различными требованиями и правилами.

Работники кибербезопасности в Великобритании должны понимать Национальный центр кибербезопасности (NCSC) и его роль в своей работе. Точно так же профессионалы в ЕС должны более тщательно учитывать GDPR во всех своих решениях. Некоторые из этих нормативных различий будут более строгими, чем то, что сотрудники увидят в США, а другие — нет. Однако они требуют адаптации.

Точно так же, как существуют корректировки стоимости жизни в конкретной стране, вероятно, также будут различия в шкале заработной платы между разными странами. Например, человек, работающий в Великобритании, будет получать другую компенсацию, чем тот, кто работает в Сингапуре. Аналогичным образом, ожидания компаний от своих партнеров по кибербезопасности немного различаются, но передовые методы обеспечения безопасности универсальны, поэтому профессионалам не нужно заново изучать, что безопасно, а что нет. Однако стандартные деловые практики и предубеждения также будут различаться, поэтому здесь могут возникнуть разные проблемы.

Например, стандартная рабочая неделя в Израиле составляет 43 часа вместо 40 и длится с воскресенья по четверг, а не с понедельника по пятницу. Иногда эти различия носят юридический характер, как, например, во Франции, где по закону большинство работников не обязаны отвечать на сообщения в нерабочее время.

Преимущества работы за границей

Адаптация к этим различиям может быть сложной, но работа за границей имеет много преимуществ. В частности, эксперты по безопасности могут зарабатывать больше в других странах. Профессионалы в некоторых странах зарабатывают в среднем шестизначную сумму, а другие могут предложить больше гибкости и преимуществ, чем компании, базирующиеся в США.

Потенциал для роста занятости и более широкий выбор возможностей трудоустройства являются другими факторами, побуждающими людей жить за границей. В США работает больше специалистов по кибербезопасности, чем где-либо еще, но во всем мире спрос остается высоким. В Великобритании, Бразилии, Южной Корее и Японии бурно развиваются отрасли безопасности, которые могут предоставить соискателям уникальные возможности.

Другие работники могут искать работу в сфере безопасности за границей просто потому, что хотят увидеть мир. В некоторых странах также может быть более низкий уровень преступности или более простые налоговые правила, чем в США.

Проблемы работы за границей

Работа за границей также принесет уникальные проблемы. Люди, которые переезжают куда-то с другим основным языком, могут столкнуться с коммуникативными барьерами.

Требуемые навыки и опыт также могут различаться в зависимости от страны. Навыки, которые составляют квалифицированного эксперта по кибербезопасности в США, могут не иметь такого же признания в Японии, поэтому некоторые работники могут столкнуться с ограниченными возможностями при переезде за границу.

Путешествующие сотрудники службы безопасности, решившие работать удаленно, столкнутся с некоторыми собственными проблемами кибербезопасности. Они должны не забывать следовать лучшим методам обеспечения безопасности гибридной среды, чтобы сохранить конфиденциальность своих данных.

Где лучшие места для работы?

Каждая страна предлагает уникальные преимущества и недостатки для специалистов по кибербезопасности, работающих за границей. То, что представляет собой лучшее место для работы, может различаться в зависимости от предпочтений и потребностей людей, но, вообще говоря, некоторые области лучше подходят для кибербезопасности, чем другие.

В Индии быстро развиваются ИТ и банковское дело, что создает множество возможностей для специалистов по кибербезопасности. Швейцария также имеет высокий спрос на сотрудников службы безопасности благодаря своей банковской отрасли, а также привлекательна низкая налоговая ставка. У ЕС есть много возможностей, поскольку законодательство, такое как Европейский закон о кибербезопасности и GDPR, повышает спрос на специалистов по безопасности. Если вы работаете за границей, очень важно понимать налоговые последствия, прежде чем брать на себя обязательства.

Некоторые работники могут мигрировать в районы с более высокой средней заработной платой. В Люксембурге самая высокая средняя заработная плата специалистов по кибербезопасности — более 110 000 долларов в год, но здесь также высокая стоимость жизни. Япония, Бельгия и Великобритания также предлагают лучшие в мире зарплаты для сотрудников службы безопасности.

Возможна ли удаленная работа в кибербезопасности?

Некоторые специалисты по кибербезопасности могут стремиться работать удаленно. Удаленная работа позволяет сотрудникам жить там, где они хотят, и открывает двери для новых возможностей, так что это отличная стратегия для работы за границей.

Эксперты прогнозируют, что в ближайшее время 25% всех рабочих мест будут удалены, но эта тенденция неравномерна в разных отраслях. Естественно, удаленных должностей на производстве меньше, чем должностей программистов. Специалисты по кибербезопасности, которые хотят работать за границей, могут задаться вопросом, где эта отрасль находится в этом спектре.

Многие должности в области кибербезопасности по-прежнему требуют, чтобы сотрудники хотя бы часть времени находились в офисе, но также доступны несколько удаленных рабочих мест. Компании становятся менее строгими в отношении некритических требований из-за глобальной нехватки специалистов по кибербезопасности в 2,7 миллиона человек. Чтобы удовлетворить этот растущий спрос, все больше сотрудников принимают удаленные и гибридные службы безопасности.

Кибербезопасность — расширяющаяся область во всем мире

Кибербезопасность — это глобальная проблема, поэтому спрос на этих работников есть во всем мире. Профессионалы, ищущие другой опыт, новые условия или потенциально более высокую заработную плату, могут извлечь выгоду из этого движения, работая за границей.

Эксперты по безопасности, которые хотят работать в международной компании, будь то в стране постоянного нахождения этой компании или удаленно, должны ожидать различий в заработной плате, культуре и даже рабочем времени. Если они смогут адаптироваться к этим уникальным соображениям, они смогут преуспеть в этой всемирно важной профессии». ***(Dylan Berger. Working Abroad as a Cybersecurity Professional: What You Need to Know // Tripwire, Inc. (https://www.tripwire.com/state-of-security/security-data-protection/working-abroad-cybersecurity-professional/). 07.09.2022).***

***

«Растущая конкуренция на рынке широкополосного доступа, граничных вычислений с множественным доступом и частных сотовых сетей, а также спрос на управление рисками кибербезопасности в эпоху 5G набирают обороты в телекоммуникациях. В результате операторам мобильной связи стало жизненно необходимо поддерживать свою инфраструктуру, чтобы их бизнес был прибыльным и безопасным. Имея это в виду, тема кибербезопасности оказывается важной для телекоммуникаций по нескольким причинам. Во-первых, эти операторы хранят огромные объемы персональных данных и несут ответственность за стабильность предоставляемых ими услуг связи. Нарушение данных или отказ службы в результате кибератаки может привести к серьезному финансовому и репутационному ущербу или повлиять на клиентов. В условиях высококонкурентного рынка это тяжелый удар для любой компании.

Кроме того, операторы связи могут предлагать дополнительные услуги безопасности в дополнение к своим базовым предложениям для создания новых источников дохода, включая облачную безопасность, фильтрацию трафика, услуги на основе SD-WAN и даже центр управления безопасностью (SOC). В этом случае зрелость операторов в области кибербезопасности может повлиять на качество услуг безопасности, которые они предоставляют своим клиентам.

Чтобы обеспечить готовность обеспечить качественную защиту и безопасность, телекоммуникационная компания должна решить проблемы кибербезопасности, связанные с ее собственной ИТ-инфраструктурой, оборудованием, услугами и данными клиентов.

Проблемы кибербезопасности

Данные, которые операторы связи собирают у своих клиентов, включают конфиденциальную личную информацию (PII), а также данные о поведении пользователей, IP-адреса, журналы и многое другое. Если произойдет нарушение, новости могут стать достоянием общественности, как только соответствующие данные о клиентах станут доступны в даркнете.

Операторы предлагают своим клиентам различные услуги, от телекоммуникаций и подключения к Интернету до облачных вычислений и веб-хостинга, среди прочего, что делает атаки на цепочки поставок еще одной серьезной

проблемой для отрасли. Если услуга оператора скомпрометирована, злоумышленники могут получить доступ ко всей инфраструктуре своих клиентов.

Это делает телекоммуникации привлекательной мишенью для APT и целевых атак. В 2021 году на каждые 10 000 рабочих станций в телекоммуникационных компаниях приходилось 79 мощных атак. Для сравнения, 70 APT атаковали ИТ-компании, 57 атаковали государственные учреждения и только 26 атаковали банковские учреждения. DDoS-атаки — еще одна проблема для телекоммуникаций. Одна из последних таких атак на интернет-провайдера в Андорре во время турнира по Minecraft. В результате связь упала по всей стране.

Неисправленное сетевое оборудование, такое как маршрутизаторы, коммутаторы, терминалы и беспроводные устройства, может стать точкой взлома. Через уязвимости на этих устройствах преступники могут получить доступ к сети и трафику организации или запустить атаку «человек посередине». Ранее в этом году злоумышленники пытались использовать старые уязвимости, обнаруженные в неисправленных устройствах нескольких производителей, пытаясь получить доступ к сети оператора связи.

Принципы защиты, о которых следует помнить телекоммуникационным компаниям

Стандартные меры защиты предприятия должны охватывать всю инфраструктуру телекоммуникационной компании, включая все конечные точки, серверы, центры обработки данных и виртуализированные инфраструктуры, а также сети и любое сетевое оборудование. Команда ИТ-безопасности компании должна знать каждый угол своей сети и оценивать риски всех возможных атак через различные точки входа.

Защита конечных точек с возможностями обнаружения и реагирования является обязательной. Когда дело доходит до целенаправленных атак, задача группы безопасности состоит в том, чтобы распознать признаки атаки, независимо от того, насколько они скрыты. Для обнаружения атак на сетевом уровне и предотвращения распространения атаки со скомпрометированного оборудования необходим анализ сетевого трафика. Система обнаружения вторжений помогает обнаруживать признаки атаки в сетевом трафике и позволяет пользователям обнаруживать весь путь угрозы, чтобы вовремя ее остановить.

Необходимы дополнительные меры для обеспечения того, чтобы сетевые устройства, используемые в инфраструктуре самим оператором или клиентами, не становились частью ботнета и DDoS. Это может произойти из-за неисправленных устройств или из-за слабых паролей или паролей по умолчанию на пользовательских маршрутизаторах. Оператору связи необходимо постоянно обновлять все свое оборудование до последних версий и изолировать пользовательские устройства, чтобы к ним не было доступа с лишних портов. Кроме того, необходимо отслеживать трафик, чтобы убедиться в отсутствии избыточного трафика ICMP или DNS от этих устройств.

Учитывая все это, для телекоммуникационных компаний нет лучшего времени, чем сегодня, чтобы проанализировать состояние своей кибербезопасности. Зрелая защита от кибербезопасности будет способствовать стабильному бизнесу оператора и облегчит путь к новым бизнес-возможностям, сохраняя при этом

безопасность и защиту текущих пользователей». ***(Lisa Kilpatrick. Why the Telecom Industry Must Prioritize Cybersecurity // Techstrong Group Inc. (https://securityboulevard.com/2022/09/why-the-telecom-industry-must-prioritize-cybersecurity/). 08.09.2022).***

***

«Безопасность электронной почты является одним из основополагающих аспектов протоколов безопасности организации, потому что это то, что потенциально может предотвратить многие угрозы. Несмотря на то, что это так, наиболее распространенные методы обеспечения безопасности электронной почты, по-видимому, не защищают организации, которые их используют: за последний год 89% из них пострадали от взлома электронной почты.

Эти данные взяты из опроса, проведенного Osterman Research по просьбе Cyren. После всего сказанного важно отметить, что многие компании, использующие Microsoft 365, участвовали в этом опросе, поэтому его результаты считаются довольно точными. Чуть менее половины организаций заявили, что их протоколы безопасности эффективны, и такое же число считают, что они могут успешно противостоять потенциальным угрозам, которые могут быть нацелены на их почтовые серверы.

Более того, общее количество взломов этого типа более чем удвоилось менее чем за три года, при этом текущие цифры вдвое превышают показатели 2019 года, если учесть все обстоятельства. Действительно тревожным фактом в этом отчете является то, что 99% организаций обучают своих пользователей выявлять подозрительные электронные письма и помечать их, но уязвимости по-прежнему используются, несмотря на то, что они вкладывают средства в частое обучение сотрудников.

Это может быть связано с тем, что организации анализируют только четверть помеченных электронных писем, что указывает на то, что они не заходят слишком далеко за рамки стандартных действий, которые они знают. Организации должны быть более активными в таких вещах, потому что независимо от того, сколько подозрительных электронных писем укажут их сотрудники, эти системы не повлияют на повышение безопасности, если организации не будут играть свою роль, анализируя указанные электронные письма и просматривая их. в то, как эти угрозы, возможно, сработали. Использование только базовых протоколов безопасности является причиной того, что эти угрозы продолжают оставаться распространенными». ***(Zia Muhammad. Common Email Security Practices Called Into Question as 89% of Organizations Suffered Breaches In the Past Year // Digital Information World (https://www.digitalinformationworld.com/2022/09/common-email-security-practices-called.html). 08.09.2022).***

***

Исследование, проведенное ThriveDX Enterprise, показывает, что осведомленность о кибербезопасности среди организаций по всему миру возросла до 97%.

Естественно, повышение осведомленности о кибербезопасности — это не то же самое, что полное оснащение для устранения нарушений кибербезопасности, но всегда приятно видеть прогресс. Честно говоря, такого рода продвижение крайне необходимо и давно назрело; Киберпреступники всегда были на несколько шагов впереди с точки зрения использования старых уязвимостей и выявления новых в системах безопасности. Мы слышим о взломе почти ежедневно, независимо от того, были ли они совершены с помощью серьезной защиты или с использованием одного незадачливого сотрудника, работающего в крупной организации. В любом случае, какое-то осознание давно было необходимо, и мы должны быть просто рады, что оно уже в пути.

Прошлые исследования показали, что многие нарушения кибербезопасности совершаются путем использования неосведомленности сотрудников (примерно 91%, если быть точным), и поэтому в будущем закладываются основы для обучения и повышения квалификации таких людей. Конечно, когда я говорю «служащий», само собой разумеется, что высшее руководство так же непреднамеренно замешано в этих схемах, как и рядовой рабочий. Возможно, даже более того, учитывая, что такие люди обычно имеют доступ к конфиденциальной информации, которой обычно не делятся с другими людьми. 58 % всех опрошенных компаний даже внедрили информационные сессии для своих сотрудников, а 42 % даже предоставили им инструменты для противодействия потенциальным нарушениям, такие как кнопка обнаружения фишинга. 27% проводят более семи симуляций ложного фишинга каждый год, а одна пятая часть всего выборочного населения проводит не менее одной симуляции в год. Честно говоря, хотя увеличение и приятно, многие из них по-прежнему очень незначительны, и необходимо добиться дальнейшего практического прогресса.

Даже такой прогресс привел к чистому положительному эффекту, причем очень заметному. 58% опрошенных сотрудников считают, что они стали лучше осведомлены о заявлениях о миссии, политиках и показателях. 65 % также считают, что необходимо проделать гораздо больше работы с точки зрения кибербезопасности, чтобы добиться действительно существенного увеличения количества утечек». ***(Arooj Ahmed. A Research Publication Reveals That Organizations Are Becoming More Aware of Potential Cybersecurity Threats That Can Be Encountered // Digital Information World (https://www.digitalinformationworld.com/2022/09/a-research-publication-reveals-that.html). 09.09.2022).***

***

«С точки зрения поверхности атаки, старые сетевые технологии бледнеют по сравнению с современными облачными технологиями. Он хорошо известен тем, что обеспечивает прозрачность данных, извлекаемых сторонними сайтами и приложениями, а также то, как эти данные защищены и используются. Но не все с этим согласны.

В свете исследования, проведенного Snyk, поставщиком услуг безопасности и аналитической компанией, восемьдесят процентов корпораций в прошлом году столкнулись с нарушением безопасности, что привело к утечке личных данных. Это

нарушение данных указывает на то, что фирмам необходимо модернизировать способы защиты пользовательских данных и способы их обработки.

Адаптация к облачной безопасности — непростая задача. Как пояснил Сник, 78% учреждений считают, что традиционные методы устарели и больше не совместимы с облаком. С другой стороны, 93% участников опроса выразили обеспокоенность по поводу нехватки специалистов по кибербезопасности.

По словам Эндрю Райта, автора отчета, облачные технологии подталкивают разработчиков к тому, чтобы идти в ногу с современными требованиями. Эндрю также добавил, что сложности, с которыми сталкиваются облачные сети, связаны с непродуктивными мерами, принимаемыми фирмами. Почти семьдесят семь процентов компаний, принявших участие в этом исследовании, согласились, что они сталкиваются с серьезными проблемами, которые возникают из-за несовместимости между командой и инструментами, которые они используют при работе с ошибками.

Однако эти ограничения можно исправить, выполнив некоторые действия, в том числе изменив корневой код. Это можно сделать с помощью организаций ИАК, поэтому вероятность ошибки можно свести к минимуму.

Сама исследовательская группа оказывает услуги другим компаниям, предлагая им другие методы, которые помогут им перейти к облачным сетям и расширить возможности разработчиков, чтобы можно было своевременно устранять любые ошибки кодирования.

Многие организации предоставляют эти услуги, поэтому любая ошибка или проблема могут быть выявлены до того, как данные будут взломаны, что не только создает проблемы для компании, но и позволяет использовать утечку данных не по назначению». ***(Arooj Ahmed. A numbers of firms went through a massive data breach last year // Digital Information World (https://www.digitalinformationworld.com/2022/09/a-numbers-of-firms-went-through-massive.html). 16.09.2022).***

***

«Результаты отчета Vade показывают преобладание поставщиков управляемых услуг (MSP): 96% организаций либо в настоящее время передают MSP хотя бы часть своих потребностей на аутсорсинг, либо планируют делать это в будущем. В отчете также анализируются успехи и недостатки решений для защиты электронной почты, а также возможности выхода на рынок у MSP.

Опрос, проведенный Vanson Bourne, включает в себя результаты опроса 500 лиц, принимающих решения в области ИТ (ITDM) в организациях со штатом от 10 до 1000 сотрудников.

69% респондентов заявили, что серьезная брешь произошла в обход их текущего решения для защиты электронной почты, а 92% заявили, что готовы выслушать предложения по безопасности электронной почты, сделанные MSP. Это лишь одна из областей, где MSP могут помочь устранить недостатки, которые делают предприятия малого и среднего бизнеса уязвимыми для атак, и могут сыграть решающую роль в защите от самоуспокоенности.

В отчете исследуется важность кибербезопасности и основные причины, лежащие в основе этого стремления, то, как MSP могут воспользоваться

преимуществами этой растущей важности, и почему ITDM должны сосредоточить свое внимание на всех областях кибербезопасности.

«Лица, принимающие решения, согласны с тем, что кибербезопасность чрезвычайно важна, и она будет становиться все более важной по мере увеличения изощренности кибератак», — сказал Жорж Лотижье, генеральный директор Vade. «Однако мы также обнаружили, что, хотя уверенность в кибербезопасности высока, этот бычий оптимизм может быть неуместным. В прошлом году лица, принимающие решения в области ИТ, стали свидетелями большего количества атак, чем раньше».

Ключевые результаты

Значение кибербезопасности возрастает: 91 % ITDM заявили, что важность кибербезопасности будет расти в течение следующих двух лет, а 63 % назвали возросшую изощренность кибератак ключевым фактором, обуславливающим их внимание к кибербезопасности.

Время для MSP настало — 96% организаций либо в настоящее время передают MSP хотя бы часть своих потребностей на аутсорсинг, либо планируют делать это в будущем. Тремя наиболее важными услугами для них являются мониторинг угроз и вторжение (43%), консультирование по кибербезопасности (37%) и управление брандмауэром (36%).

Атаки растут — 79% ITDM согласились с тем, что количество кибератак, с которыми столкнулась их организация, увеличилось за последние 12 месяцев, в среднем за тот же период времени было совершено 8 кибератак. Вредоносное ПО (40%), взлом паролей (35%) и фишинг (34%) были наиболее распространенными кибератаками. Малые предприятия также чаще (35%), чем предприятия (11%), подвергались атакам эксплойтов нулевого дня.

Лица, принимающие решения в области кибербезопасности, по-прежнему уверены: 94 % ITDM высоко уверены в способности своей организации полностью защитить себя от всех типов атак, при этом 51 % заявили, что они полностью уверены. Однако 68% согласны с тем, что решения по обеспечению безопасности в их организациях не настолько продвинуты, как могли бы быть.

Безопасность электронной почты может быть затенена или неправильно понята — 69% ITDM заявили, что серьезное нарушение обошло их текущее решение для защиты электронной почты. 77% респондентов сообщили, что их организация использует встроенные функции безопасности, предлагаемые их поставщиком услуг электронной почты (например, Microsoft 365, G-Suite и т. д.)…» ***(MSPs and cybersecurity: The time for turning a blind eye is over // Help Net Security (https://www.helpnetsecurity.com/2022/09/12/msps-email-security/). 12.09.2022).***

***

«Kroll объявила о своем отчете «Киберриски и финансовые директора: чрезмерная уверенность дорого обходится», в котором финансовые директора (финансовые директора) были крайне невежественны в отношении кибербезопасности, несмотря на уверенность в способности своей компании отреагировать на инцидент.

Отчет, подготовленный StudioID of Industry Dive, выявил три ключевые темы среди 180 опрошенных руководителей финансового отдела по всему миру:

Неведение — это блаженство. 87% финансовых директоров уверены в том, что их организация сможет отреагировать на кибератаку. Это не соответствует уровню информированности финансовых директоров о проблемах киберрисков, учитывая, что только четверо из 10 опрошенных проводят регулярные брифинги со своими киберкомандами.

Широкомасштабные повреждения. 71% представленных организаций понесли более 5 миллионов долларов финансовых убытков в результате киберинцидентов за предыдущие 18 месяцев, а 61% за это время пострадали как минимум от трех серьезных киберинцидентов. Восемьдесят два процента руководителей, принявших участие в опросе, заявили, что их компании понесли убытки в размере 5% или более в своих оценках после крупнейшего инцидента с кибербезопасностью за последние 18 месяцев.

Увеличение инвестиций в кибербезопасность. Сорок пять процентов респондентов планируют увеличить долю своего общего ИТ-бюджета, выделяемую на информационную безопасность, как минимум на 10%.

Грег Майклс, глобальный руководитель отдела киберуправления и рисков в практике киберрисков в Kroll, сказал: «Мы часто видим, что финансовые директора недостаточно осведомлены о финансовых рисках, связанных с киберугрозами, до тех пор, пока они не столкнутся с инцидентом. На этом этапе становится ясно, что они должны участвовать не только в восстановлении, включая предоставление доступа к чрезвычайным фондам и закупку сторонних поставщиков, но также в разработке стратегии и инвестировании в киберпространство как до, так и после инцидента…» ***(CFOs' overconfidence in cybersecurity can cost millions // Help Net Security (https://www.helpnetsecurity.com/2022/09/14/cfos-cybersecurity-confidence/). 14.09.2022).***

***

«Несмотря на глобальные расходы на киберзащиту в размере более 130 миллиардов долларов США и тысячи поставщиков, которые в настоящее время активно работают на рынке кибербезопасности, среда становится все хуже, когда речь идет об угрозах безопасности.

Количество, характер и серьезность нарушений кибербезопасности продолжают расти с начала пандемии. Фактически, нарушение безопасности или атака программ-вымогателей регистрировались каждые 11 секунд до 2022 года, и 61% организаций сообщают как минимум об одной атаке каждый год.

Учитывая этот все более изощренный ландшафт угроз, современные организации пересматривают свои ожидания. Там, где стеки устаревших технологий безопасности не успевают за меняющимся ландшафтом угроз, ИТ-руководители постоянно ищут новые способы повышения уровня безопасности без необходимости начинать с нуля.

Поиск подходящего таланта для решения этой задачи является постоянной задачей. Сохраняющаяся глобальная нехватка специалистов в области кибербезопасности не собирается уменьшаться, поскольку постоянно меняющийся ландшафт угроз требует все более широкой базы знаний и навыков в области безопасности.

В результате в настоящее время миллионы вакансий во всем мире остаются незаполненными, а это, в свою очередь, создает огромный спрос, а внутренние кадровые ресурсы становятся непомерно дорогими.

Директорам по информационной безопасности нужны решения, которые обеспечат безопасность их организаций и позволят им более эффективно управлять рисками. Киберстрахование является одним из аспектов, поскольку оно обеспечивает дополнительный уровень защиты в случае атаки, позволяя руководителям службы безопасности передавать риск кибербезопасности страховой компании.

Но покрывают ли взносы по киберстрахованию все атаки программ-вымогателей и правильно ли проводят анализ пробелов директора по информационной безопасности? Учитывая все риски, связанные с киберстрахованием, требования для получения полиса становятся все более сложными, помимо значительной тенденции к увеличению стоимости защиты, которая растет в среднем на 30% в годовом исчислении, и нет никаких признаков это замедление.

Соблюдение нормативных требований и отчетность — еще одна проблема, которую директора по информационной безопасности не могут игнорировать. Чтобы пройти сертификацию и соответствовать требованиям, необходимо не только соблюдать все стандарты и правила, но и руководители службы безопасности должны обеспечить адекватную и своевременную отчетность. Так как же руководители службы безопасности могут справиться с этими проблемами? Как они могут подойти к выбору ресурсов и какие ключевые технологии позволят им использовать передовой опыт?

Системы кибербезопасности и критически важные технологии

Структура кибербезопасности NIST была разработана, чтобы направлять специалистов по ИТ-безопасности при оценке их состояния безопасности и улучшении снижения рисков. Эта структура помогает организациям убедиться, что у них есть подходящие системы для обеспечения достаточно надежного подхода к кибербезопасности.

Он охватывает пять действенных стратегий управления рисками: «выявление», «защита», «обнаружение», «реагирование» и «восстановление» после кибератаки.

Удостоверение личности

Независимо от того, где находится конечный пользователь, существуют уязвимости. В год публикуются десятки тысяч новых уязвимостей, ежедневно публикуется примерно 55 новых уязвимостей. В то время как собственные ИТ-команды могут решить только некоторые из них, около 5% представляют реальный риск — те, которые можно использовать удаленно и которые уже используются в качестве оружия.

Крайне важно оценивать, определять приоритеты и устранять наиболее важные риски для сети и бизнеса с помощью непрерывного сканирования рисков, которое обеспечивает представление обо всех активах, существующих в сетевой среде, и советует командам сосредоточиться на уязвимостях, которые больше всего подвергают эти активы риску. риск.

Защита

Благодаря стремительному развитию распределенных сетей данные сегодня живут повсюду. Обеспечение безопасного подключения и управление им «там, где оно существует» — между несколькими источниками и устройствами — является частью задачи. Там, где у специалистов по безопасности часто нет времени уделять приоритетное внимание сетевой безопасности, эти среды постоянно меняются и требуют анализа и дополнений в реальном времени.

Управляемые брандмауэры освобождают специалистов по безопасности от необходимости поддерживать наборы правил в точке входа в сеть, а также позволяют извлечь пользу из опыта более широкого круга организаций.

Еще важнее для обеспечения сетевой безопасности то, что директора по информационной безопасности нуждаются в интеллектуальном анализе сети, чтобы более целостно рассматривать поведение трафика, включая различные источники данных и автоматически определяя, что является хорошим, а что плохим трафиком.

Отсюда необходимо использовать соответствующие технологии, такие как предотвращение вторжений, сетевой антивирус и SD WAN, чтобы обеспечить безопасность всех пользователей в режиме реального времени и обеспечить беспрепятственное безопасное подключение.

Обнаружение

Сегодня у организаций больше приложений, больше данных, больше местоположений и больше удаленных пользователей, чем когда-либо прежде. Усталость от бдительности — это реальная проблема, если даже следить за каждым элементом. Миллионы ежедневных уведомлений предупреждают о потенциальных угрозах безопасности, и, хотя некоторые из них можно отбросить, другие требуют немедленного реагирования.

Управляемые решения SIEM позволяют специалистам по безопасности регистрировать события кибератак, а также проводить перекрестный анализ и собирать данные в удобном для действий формате. Они позволяют директорам по информационной безопасности быстро реагировать и приносить пользу в разгар инцидента, в то самое время, когда это необходимо, определяя, как произошло нарушение безопасности и как предотвратить причинение большего ущерба.

Ответ

Когда мы думаем о реагировании, мы на самом деле говорим об обнаружении и реагировании на управляемые конечные точки (EDR), обеспечивающем безопасность конечных точек следующего поколения, которая может быстро выявлять и останавливать ненормальное поведение. Киберпреступность становится все более изощренной, и векторы атак появляются повсюду, особенно после перехода на удаленную работу.

Конечный пользователь является самой большой уязвимостью в любой сетевой среде, и образование имеет важное значение. Но риск все еще существует, независимо от того, сколько обучения проводится, и крайне важно ежедневно активно защищать конечную точку.

Восстановление

Незапланированные простои могут привести к непоправимому и долгосрочному ущербу для организации, клиентов и репутации. Последствия

стихийного бедствия могут включать потерю доходов, отток клиентов и, в худшем случае, невозможность продолжать бизнес-операции.

Здесь восстановление требует упреждающего резервного копирования и репликации данных. Безопасное облачное резервное копирование обеспечивает простое и экономичное резервное копирование данных за пределы площадки, чтобы обеспечить передовые методы защиты 3-2-1. Служба обеспечивает надежную защиту от целого ряда случаев потери данных, включая злонамеренное или случайное удаление, аппаратные сбои и киберпреступления.

Кроме того, аварийное восстановление как услуга (DRaaS) может объединить нужных людей, процессы и технологии, чтобы подготовить бизнес к стихийным бедствиям и обеспечить быстрое и успешное восстановление.

Улучшение защиты с помощью поставщиков управляемых услуг безопасности (MSSP)

Учитывая сложность, серьезность и круглосуточный характер постоянно меняющегося ландшафта угроз, растущие требования к соблюдению нормативных требований, а также стоимость и ограничения внутренних ресурсов, правильный MSSP может предложить директорам по информационной безопасности отличное решение для удовлетворения их потребности в доступном и надежная защита от киберпреступности.

По прогнозам, к 2025 году мировой рынок управляемых услуг безопасности достигнет 356,24 млрд долларов США, поэтому очевидно, что все больше профессионалов в области безопасности, чем когда-либо, обращаются к решениям MSSP для укрепления своей защиты.

Они не только обеспечивают доступ к группе специализированных экспертов по безопасности и новейшим технологиям, но также обеспечивают такие преимущества, как экономия средств, соблюдение нормативных требований и снижение рисков, масштабируемость и доступ к инновационным технологиям.

Эти специализированные группы поддержки удовлетворяют все потребности организации в обеспечении безопасности благодаря специальным командам, современным технологиям, объектам и процессам, которые отслеживают и управляют самыми простыми и самыми сложными инцидентами безопасности.

Многие предоставят организациям помощь в разработке процесса непрерывного улучшения для защиты их бизнеса по мере того, как ландшафт угроз продолжает развиваться. Они также учитывают анализ влияния на бизнес и используют методологию определения приоритетов, чтобы определить и сосредоточиться на решении тех проблем, которые наиболее важны для организации». ***(Mark Bowen. Improving cybersecurity with Managed Security Services Providers // Intelligent CIO (https://www.intelligentcio.com/north-america/2022/09/22/improving-cybersecurity-with-managed-security-services-providers/#). 22.09.2022).***

***

«…Ранее в этом году Брюс Шнайер и Уилер в статье для The Cipher Brief сформулировали некоторые конфликты между корпоративными

финансовыми интересами и международными соглашениями о кибербезопасности. Ниже кратко изложены некоторые из их основных моментов.

Парижский призыв к доверию и стабильности в киберпространстве был инициативой президента Франции Эммануэля Макрона во время Форума ЮНЕСКО по управлению интернетом в 2018 году. Это попытка правительств мира собраться вместе и создать набор международных норм и стандартов для надежного, заслуживающего доверия, безопасного и защищенного Интернета.

Это не международный договор, но он налагает обязательства на стороны, подписавшие его. Это важная веха для глобальной безопасности и безопасности в Интернете. Корпоративные интересы присутствовали во всей этой инициативе, спонсируя и управляя различными частями процесса.

В рамках конкурса французская компания Cigref и российская компания «Лаборатория Касперского» возглавили рабочую группу по процессам кибербезопасности вместе с французским исследовательским центром GEODE. Еще одну рабочую группу по международным нормам возглавляли американская компания Microsoft и финская компания FSecure, а также исследовательский центр Флорентийского университета.

Список участников третьей рабочей группы включает больше корпораций, чем любая другая группа. В результате этот процесс стал сильно отличаться от предыдущих международных переговоров. Вместо того, чтобы правительства объединялись для создания стандартов, им руководят те самые корпорации, которыми должен управлять новый международный климат регулирования.

Это не правильно. Компании, производящие регулируемые инструменты и оборудование, не должны вести переговоры о международном нормативном климате, а их руководители не должны назначаться на ключевые роли в переговорах без назначения и подтверждения.

Это отказ США и других правительств, в основном западных, от ответственности за что-то, что слишком важно, чтобы с ним обращались так высокомерно. С одной стороны, в этом нет ничего удивительного. Понятия доверия и стабильности в киберпространстве касаются гораздо большего, чем международная безопасность.

Они касаются доли рынка и корпоративной прибыли. И корпорации уже давно ведут политиков на быстро меняющемся и высокотехнологичном поле битвы, которое представляет собой киберпространство.

Глобальный Интернет всегда опирался на то, что известно как модель с участием многих заинтересованных сторон, когда те, кто появляется и выполняет работу, могут иметь большее влияние, чем те, кто отвечает за правительства.

Инженерная рабочая группа Интернета (IETF), группа, которая согласовывает технические протоколы, обеспечивающие работу Интернета, в основном управляется добровольцами.

Лучше всего это работало в эпоху благополучного забвения Интернета, когда никто, кроме технологов, не заботился об этом. Сегодня все по-другому. Корпоративные и государственные интересы доминируют, даже если вовлеченные лица используют вежливую выдумку своих имен и личностей.

Однако мы далеки от прошлых десятилетий, когда Интернет был чем-то, что правительства не понимали и в значительной степени игнорировали.

Сегодня Интернет представляет собой важнейшую инфраструктуру, лежащую в основе большей части общества, а его структура управления глубоко волнует нации.

Привлечение коммерческих технологических компаний к участию в процессе Парижского соглашения по регулированию технологий аналогично передаче оборонным подрядчикам Northrop Grumman или Boeing ответственности за ядерные соглашения ОСВ 1970-х годов между США и Советским Союзом.

Это также не первый случай, когда американские корпорации возглавляют то, что должно быть процессом международных отношений в отношении Интернета. С тех пор как он впервые выступил на эту тему в 2017 году, президент Microsoft Брэд Смит стал почти синонимом термина «Цифровая Женевская конвенция».

Дело не только в том, что корпорации в США и других странах берут на себя ведущую роль в международной дипломатии; они сводят дискуссию к словам и понятиям. Почему это происходит? В разных странах есть свои проблемы, но мы можем указать на несколько, которые в настоящее время досаждают правительствам.

Прежде всего, «кибер» до сих пор не воспринимается всерьез большинством правительств. Это нереально для пожилых военных ветеранов или еще более пожилых политиков, которые путают Facebook с TikTok и используют один и тот же пароль для всего.

Это даже не тема для переговоров торговых представителей. Ядерное оружие или оружие массового уничтожения, разоружение, терроризм, изменение климата, незаконный оборот наркотиков или торговля людьми — это «настоящая геополитика», в то время как Интернет и киберпространство до сих пор считаются смутно волшебными, и что-то, что можно «исправить», кретины выдергивают шнуры питания из стен, блокируют/фильтруют Facebook, любое другое приложение или даже сам доступ в Интернет! Есть даже степени контроля.

В США, например, кажется, что в самом сердце правительства США идет постоянная борьба за власть, связанная с кибер-проблемами, между Белым домом, Министерством внутренней безопасности (представленным CISA) и военными (представленными Киберкомандованием США).

Попытка создать еще один киберцентр власти внутри Государственного департамента угрожает этим существующим полномочиям.

Легче оставить это в руках частного бизнеса, который не влияет на бюджет или территорию этих государственных организаций. Легче обвинять, когда что-то идет наперекосяк, что часто бывает, пока не заметут под ковер и не замажут расследованиями, отложенными после того, как вся суета утихнет. В конце концов, это редкость быть на первых полосах новостей дольше нескольких дней.

Мы не хотим возвращаться к эпохе, когда только правительства устанавливали технологические стандарты.

Модель управления времен телефона — еще один урок того, как не надо делать.

Международный союз электросвязи (МСЭ) является агентством, управляемым Организацией Объединенных Наций.

Он умирает и тяжеловесен именно потому, что им управляют национальные правительства, а гражданское общество и корпорации в значительной степени отчуждены от процессов принятия решений.

Сегодня Интернет имеет основополагающее значение для глобального общества. Это часть всего.

Это влияет на национальную безопасность и уже является неотъемлемой частью войны, как это происходит сегодня на Украине. То, как люди, корпорации и правительства действуют в киберпространстве, имеет решающее значение для нашего будущего. Интернет является критической инфраструктурой. Он обеспечивает и контролирует доступ к здравоохранению, вооруженным силам, воде, энергии, образованию и ядерному оружию.

Как это регулируется, это не просто то, что повлияет на будущее. Это будущее. С тех пор как Парижский призыв был завершен в 2018 году, его подписала 81 страна, включая США в 2021 году, 36 местных органов власти и органов государственной власти, 706 компаний и частных организаций и 390 групп гражданского общества.

Парижский призыв — не первое международное соглашение, которое ставит компании в равное положение с правительствами. Глобальный интернет-форум по борьбе с терроризмом и Крайстчерчский призыв к ликвидации экстремистского контента в Интернете делают то же самое. Но Парижский звонок отличается. Это больше.

Это важнее. Это то, что должно быть прерогативой правительств, а не средством корпоративной власти и прибыли.

Когда что-то столь же важное, как Парижский призыв, произойдет снова, возможно, на переговорах ООН по соглашению о киберпреступности, мы призываем к тому, чтобы за столом переговоров сидели настоящие правительственные чиновники с техническими знаниями, а интересы их страны были поставлены на карту… а не люди с акциями. защищать. Остается только надеяться, что здравый смысл восторжествует.

Как отметил социальный и экономический теоретик Джереми Рифкин о политическом влиянии Интернета сегодня: «Мы пришли к открытию того, что, как мы подозреваем, является новым политическим мышлением, формирующимся среди молодого поколения политических лидеров, привыкших к интернет-коммуникациям.

Их политика в меньшей степени связана с правыми и левыми, а в большей — с централизованной и авторитарной, а не с распределенной и совместной». Да благословит Бог и оставайтесь в безопасности как в цифровом, так и в физическом мире». ***(Ilaitia Tuisawau. Cyberspace in geopolitics – International cybersecurity agreements // Fiji Times Limited (https://www.fijitimes.com/cyberspace-in-geopolitics-international-cybersecurity-agreements/). 24.09.2022).***

***

«Кибербезопасность органично вошла в повседневную жизнь. Из-за вызывающего тревогу роста числа кибератак специалистам по

кибербезопасности стало трудно выбирать подходящие контрмеры с самого начала проекта, чтобы не было задержек по мере его продвижения к завершению.

Это стало этапом тестирования для лидеров кибербезопасности, поскольку стратегическое планирование стало иметь первостепенное значение для защиты активов своей организации. Стратегическое планирование — это не краткосрочная цель, которую нужно разработать. Тем не менее, это конечная цель, которую необходимо обсудить для реализации стратегий безопасности на ближайшие годы.

Ниже приведены несколько пунктов, определяющих приоритетность предположений лидеров кибербезопасности:

Прогнозы рынка кибербезопасности. Согласно прогнозам, рынок кибербезопасности вырастет с 240,27 млрд долларов США в 2022 году до 345,38 млрд долларов США в 2026 году, а совокупный годовой темп роста (CAGR) составит 9,5% в 2022–2026 годах, чтобы соответствовать мировому валовому внутреннему продукта (ВВП).

Акцент на Глобальном индексе кибербезопасности (GCI): Глобальный индекс кибербезопасности, известный ресурс, который оценивает приверженность стран кибербезопасности и поощряет действия по созданию безопасных цифровых экосистем, необходимых для восстановления и прогресса, публикуется Международным союзом электросвязи (МСЭ). Лидерам необходимо тщательное планирование, чтобы импровизировать текущий индекс GCI своей страны.

Пропаганда национальных структур управления: принятие национальной политики управления данными, направленной на повышение доступности, качества и использования данных в соответствии с возникающими и существующими технологическими потребностями десятилетия.

Права сотрудников на неприкосновенность частной жизни

Правила и методы компании по сбору, использованию и раскрытию личной информации о прошлых, настоящих или потенциальных работниках изложены в документе о политике конфиденциальности сотрудников. Некоторые компоненты политики конфиденциальности могут требоваться трудовым законодательством, в то время как другие могут быть уникальными для конкретной организации. Правила, обеспечивающие права сотрудников на неприкосновенность частной жизни, должны соответствовать глобальному ВВП.

Применение Security Service Edge (SSE)

SSE формирует опору для лучшего мониторинга и улучшения безопасности. Поскольку организации имеют дело со многими сторонними приложениями, поставщиками и удаленными работниками, безопасный и надежный способ подключения и доступа к приложениям является серьезной проблемой. К 2025 году все больше предприятий будут использовать стратегию объединения Интернета, доступа к облачным сервисам и связанным с ними частным приложениям через SSE одного поставщика.

Использование моделей нулевого доверия

По мере роста организации взаимодействия внутри и за пределами сферы также увеличиваются. Стало очевидным контролировать и отслеживать каждое взаимодействие, происходящее внутри и за пределами организации. Использование

модели нулевого доверия становится важным как просчитанная стратегия кибербезопасности, которая защищает компанию, устраняя неявное доверие и постоянно подтверждая каждый этап цифровой транзакции.

Защита сред операционных технологий (OT)

Злоумышленники запустили несколько атак на OT, в том числе на аппаратное и программное обеспечение, используемое для отслеживания и мониторинга промышленных систем управления, активов и других операций. Вместо того, чтобы беспокоиться о краже информации, лидеры кибербезопасности в этой области должны сосредоточиться на реальных рисках для людей и окружающей среды.

Планирование непрерывности бизнеса (BCP)

Из-за внезапной пандемии многие организации разорились из-за плохого планирования. Когда происходит крупномасштабный сбой, бизнес должен продолжаться без помех. Создание стратегии устойчивости для поддержки планирования непрерывности бизнеса важно для снижения подверженности пандемическим атакам.

Подотчетность

Новая норма рассматривает кибербезопасность как бизнес-риск, а не как простую техническую ИТ-проблему, поскольку она препятствует прогрессу и репутации. По мнению Gartner, участие топ-менеджеров должно быть обязательным и отражаться в их трудовых договорах.

Привычное действие

Организации должны распространять информацию с помощью игр, кампаний, досок объявлений, вебинаров и т. д., чтобы среди сотрудников стало привычкой внедрять кибербезопасность в культуру организации.

Это стратегии, которые необходимо включить на политический уровень, а затем реализовать в ближайшие месяцы. Дайте нам знать в комментариях, если мы пропустили что-то еще». ***(Swarnalatha Devarakonda. How cybersecurity leaders can build strategic planning assumptions into security strategies for next 2 years // Cyber Media (India) Ltd. (https://www.dqindia.com/how-cybersecurity-leaders-can-build-strategic-planning-assumptions-into-security-strategies-for-next-2-years/). 22.09.2022).***

***

«Согласно исследованию приоритетов безопасности Foundry за 2022 год, подавляющее большинство (90%) руководителей служб безопасности считают, что их организация не справляется с рисками кибербезопасности. Опрошенные столкнулись с этими ловушками из-за разных проблем, таких как убеждение в серьезности риска для всей или части их организации (27%) и уверенность в том, что их организация не инвестирует достаточно ресурсов для устранения рисков (26%).

Бюджеты также продолжают играть важную роль в усилиях компании по обеспечению кибербезопасности. Для малого бизнеса бюджет безопасности подскочил до 16 миллионов долларов с 11 миллионов долларов в прошлом году и 5,5 миллионов долларов в 2020 году. Бюджет предприятий остается стабильным — 122 миллиона долларов в этом году по сравнению со 123 миллионами долларов в 2021 году.

Что касается киберстрахования, растущего сектора, то около четверти организаций заявили, что имеют в виду киберстрахование, и только 23% не заинтересованы в этом.

Киберпреступность как услуга

Чтобы справиться с растущими инновациями киберпреступников и появлением различных моделей «киберпреступность как услуга», лица, принимающие решения в области безопасности, исследуют и тестируют широкий спектр новых технологий безопасности, чтобы добавить их в свой технический стек. К наиболее активно изучаемым технологиям относятся:

Организация безопасности, автоматизация и реагирование (SOAR) (34%)

Технологии нулевого доверия (32%)

Периферия службы безопасного доступа (SASE) (32%)

Технологии обмана (30%)

Брокеры программ-вымогателей (30%)

Данные ясно показывают, что по мере того, как компании растут и масштабируют свои усилия по обеспечению безопасности в тандеме, соответствующие инвестиции и бюджетные требования должны соответствовать этому. Организации всех размеров осознают риски безопасности и понимают последствия, которые могут возникнуть из-за взлома, и многие руководители служб безопасности готовятся к наихудшему сценарию. Это дает поставщикам технологий возможность лучше понять основные проблемы и предоставить соответствующие инструменты и решения.

Исследование также показывает, что нехватка навыков безопасности по-прежнему сказывается на значительной части организаций. Чтобы решить эту проблему, почти половина (45%) ИТ-руководителей просят нынешних сотрудников взять на себя больше обязанностей и использовать технологии, которые автоматизируют приоритеты безопасности. 42% отдают функции безопасности на аутсорсинг, а 36% увеличивают компенсацию и улучшают льготы.

По мере того, как лидеры в области безопасности ориентируются на конкурентоспособную рабочую силу, они также обращаются к своим партнерам по технологиям безопасности для создания более эффективных и автоматизированных методов, которые имеют смысл для их бизнеса и сотрудников.

Методология

Исследование приоритетов безопасности на 2022 год проводилось с помощью онлайн-анкетирования с июня по август 2022 года. Всего было собрано 872 респондента, занимающих руководящие должности в сфере ИТ и/или корпоративной безопасности, из регионов Северной Америки (55%), Европы, Ближнего Востока и Африки (18%) и Азиатско-Тихоокеанского региона (27%). Наиболее представленные отрасли включают технологии (25%), производство (13%), правительство/некоммерческие организации (10%) и финансовые услуги (8%). Средний размер компании составлял 10 991 человек…» ***(Report: 90% of orgs believe cybersecurity risk isn't being addressed // VentureBeat (https://venturebeat.com/security/report-90-of-orgs-believe-cybersecurity-risk-isnt-being-addressed/). 23.09.2022).***

***

«…Кибербезопасность и аббревиатуры идут рука об руку, как арахисовое масло и желе. Трудно представить одно без другого. Новые технологии неизбежно порождают новые термины, за которыми нужно следить.

Тем не менее, постоянно растущий в отрасли набор аббревиатур из аббревиатур и жаргона может затруднить сравнение технологий с течением времени. Возьмем в качестве примера три тесно связанных категории технологий обнаружения угроз: сетевое обнаружение и реагирование (NDR), обнаружение и реагирование на конечных точках (EDR) и расширенное обнаружение и реагирование (XDR). Каждый из них предлагает комплексное решение для обнаружения различных кибератак и реагирования на них. Более того, они опираются на схожие, но разные подходы, заслуживающие внимания, поскольку объем и изощренность атак продолжают расти, а риски для организаций не ослабевают.

В последние годы появились десятки поставщиков XDR. Но заслуживают ли они такой шумихи? И отличается ли XDR от технологий EDR или NDR, на которые уже полагаются тысячи организаций по всему миру? В этой статье мы сравним эти другие технологии и то, как они вписываются в современный стек кибербезопасности организации.

Системы EDR стали популярными около десяти лет назад, потому что они обещали более целостный подход к обнаружению нарушений безопасности по мере их возникновения. Самые старые технологии обнаружения угроз, описанные выше, системы EDR защищают компании, развертывая программный агент на каждом подключенном конечном устройстве. Эти агенты конечных точек могут помочь обнаруживать вредоносные действия, ранее пропущенные брандмауэром, например, путем выявления ощутимых изменений, таких как изменения реестра и манипулирование файлами ключей.

Для многих компаний EDR имеет решающее значение для их общего состояния кибербезопасности. Более продвинутые системы EDR могут автоматически использовать машинное обучение или ИИ для обнаружения новых угроз, используя профили, основанные на подозрительном поведении и активности. Кроме того, специалисты по безопасности могут просмотреть данные конечных точек, чтобы определить потенциальные точки компрометации.

Однако существуют пределы их эффективности. Например, журналы обнаружения EDR не всегда вызывают оповещения, поэтому для предотвращения кибератак может потребоваться периодическая ручная проверка данных конечных точек. Агенты также не могут быть развернуты на всех устройствах (например, устройствах BYOD или IoT) или в таких средах, как общедоступное облако, что может привести к появлению пробелов в видимости, которыми могут воспользоваться злоумышленники.

Многие специалисты могут подумать, что в случае кибератаки субъекту угрозы придется скомпрометировать конечную точку и, таким образом, его можно будет обнаружить. Тем не менее, по мере того, как вредоносное ПО и злоумышленники становятся более компетентными, они могут маскировать начальные признаки атаки или даже перехватывать агент и спать до тех пор, пока он

не понадобится. Эти пробелы разрушают миф о том, что организациям нужен только EDR. А поскольку все больше сотрудников работают удаленно и в гибридных средах, организациям требуется более универсальная и передовая технология для обнаружения угроз в различных средах, поэтому многие организации обращают внимание на решения XDR.

Хотя определения меняются по мере развития категории, XDR обычно понимается как следующая эволюция EDR, ставшая более эффективной за счет интеграции сетевых, прикладных и облачных источников данных для более быстрого и эффективного реагирования на угрозы. Конечно, отчасти причина такой путаницы в отношении возможностей платформ XDR и различных определений заключается в том, что существуют разные типы.

В целом существует три типа платформ XDR:

Родной (работает только с продуктами одного поставщика)

Открытый (работает со всеми поставщиками)

Гибрид (может интегрировать данные от некоторых внешних поставщиков с ограничениями)

В отличие от EDR, решения XDR пытаются реализовать более проактивный подход к обнаружению угроз и реагированию на них, предоставляя решение на одной платформе, обеспечивающее видимость нескольких потоков данных (конечных точек, сети и облака). Кроме того, эту аналитику можно дополнительно улучшить с помощью расширенных инструментов управления информацией и событиями безопасности (SIEM) и оркестрации безопасности, автоматизации и реагирования (SOAR) при использовании аналитики и автоматизации для решения более сложных проблем и угроз.

Хотя одноплатформенный подход XDR подходит организациям с разнообразными средами данных для мониторинга всей деятельности в одном месте, даже оптимизированное одноплатформенное решение имеет ограничения, если ему не хватает видимости в более широкой сетевой среде организации. Руководителям кибербезопасности необходимо видеть изменения в сетевой активности и сравнивать их с данными конечных точек и облачными данными, где решения NDR могут предоставить необходимый контекст, чтобы сосредоточиться на потенциальных киберугрозах.

В отличие от решений EDR или XDR, NDR фокусируется на анализе пакетных данных в сетевом трафике, а не на конечных точках или других потоках данных для обнаружения потенциальных киберугроз. В конце концов, пакеты не лгут, что делает их лучшим источником надежной, точной и всесторонней информации. А за счет объединения NDR с другими решениями, такими как инструменты анализа журналов с помощью системы управления информацией и событиями безопасности (SIEM) и EDR, организации могут устранить мертвые зоны в своих сетях. Вместе решения NDR повышают возможности безопасности, предоставляя сетевой контекст и автоматизируя реагирование на угрозы, поддерживая более тесное сотрудничество между сетевыми командами и группами безопасности и более быстрое устранение угроз.

Однако в рамках категории отчетов о недоставке важно различать возможности более продвинутых платформ, которые предлагают функции, которые

должны включать современные стеки кибербезопасности. Например, оценка различных отчетов о недоставке гарантирует, что они могут обеспечить надежную криминалистическую экспертизу с долгосрочным хранением данных. Также очень важно, что они не полагаются на данные на основе NetFlow, которые поддерживаются не во всех средах и могут открывать возможности для более сложных атак, зависящих от туннелирования. Действительно, более продвинутые системы должны позволять задним числом просматривать сетевой трафик для изучения поведения угроз до, во время и после атак. Таким образом, при обнаружении индикатора компрометации (IOC) группы безопасности могут исследовать связь скомпрометированных хостов, определить боковое перемещение и определить, произошла ли утечка данных.

Таким образом, EDR предназначены для мониторинга и смягчения атак на конечные точки через подключенные компьютеры и серверы, но только там, где могут быть развернуты агенты. В результате EDR не работает, например, в некоторых облачных средах хостинга. Напротив, отчеты XDR предлагают более унифицированный платформенный подход к мониторингу устройств и потоков данных, но часто не имеют сетевого контекста, который отчеты о недоставке обеспечивают посредством мониторинга пакетов в реальном времени.

Реальность такова, что большинству крупных организаций сегодня требуется более комплексное решение, которое объединяет данные сети и конечных точек с другими решениями по обеспечению безопасности для получения более надежного представления в режиме реального времени о постоянно меняющемся ландшафте угроз. Таким образом, сетевые данные, предоставляемые расширенными отчетами о недоставке, служат связующим звеном, соединяющим и контекстуализирующим входные данные от дополнительных систем EDR, XDR, SIEM и SOAR, что делает их более эффективными для более быстрого обнаружения угроз и реагирования на них. Ведь скрыть свои следы в сети невозможно, а кибератаки только усложняются. Работая в тандеме, эти системы обеспечивают полное представление о поведении злоумышленника и индикаторах компрометации». ***(Mark Doering. NDR vs. EDR vs. XDR — Which Is Right for Your Cybersecurity Stack? // Spiceworks Inc. (https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/ndr-vs-edr-vs-xdr-the-right-cybersecurity-stack/). 27.09.2022).***

***

«Кибербезопасность была «горячей проблемой» в течение многих лет. Компании знают, что существуют значительные риски, но не имеют никакого метода для расчета своих бюджетных приоритетов. Средства массовой информации продолжают публиковать обширную статистику киберпреступлений, а члены правления ломают голову, задаваясь вопросом, на чем им следует сосредоточиться в отношении кибербезопасности. Тем не менее, индустрия еще не поняла, как стратегически оформить этот разговор.

Изменения на страховом рынке, стремительный рост преступной деятельности и расширенная нормативно-правовая база вскоре прояснят коммерческую ценность кибербезопасности, поскольку она начнет стоить реальных денег. Компании защищают себя от соблюдения нормативных требований и рисков непрерывности

бизнеса, отдавая их на аутсорсинг посредством страхования. К сожалению, страховщики обнаружили, что коэффициент убыточности в киберстраховании во многих случаях составляет почти 110%. Кроме того, поскольку хакеры нацелены на интеллектуальную собственность и инфраструктуру страны, регулирующие органы и законодатели предлагают новые требования для устранения подверженности США риску на публичных рынках и в критической инфраструктуре. В результате компании будут напрямую нести бремя увеличения нормативных штрафов из-за расширения требований соответствия.

Рыночные и политические тенденции заставляют выбирать инфраструктуру безопасности

Сегодня рынок киберстрахования оценивается в 14,5 миллиардов долларов. К сожалению, данных о киберрисках мало, и актуарии не смогли успешно количественно оценить их стоимость. Страховые компании безуспешно строили свои предположения и несли значительные убытки. В результате перевозчики повышают тарифы в этом году на 174%, ужесточают условия и расширяют исключения. Например, компания Lloyds of London только что объявила, что исключит из своей киберстраховки все акты войны, связанные с деятельностью национального государства, и что война не обязательно должна быть объявлена. Время для этого изменения не могло быть хуже, потому что ФБР и MI5 совместно предупредили о хакерских атаках Китая на интеллектуальную собственность США в 2022 году. В результате стоимость киберстрахования быстро растет, покрытие становится более ограниченным,

Статистика ФБР показывает, что киберпреступность выросла более чем на 300% с начала пандемии. Киберпреступники становятся все более изощренными и используют украденные данные для создания списков целей для будущих каскадных атак. Это акцентирует риски для предприятий, их клиентов и поставщиков. Например, в период с 2018 по 2020 год хакеры украли около 26 миллионов учетных данных пользователей, расширив свой след преступления. Кроме того, в 2021 году 34% всех предприятий пострадали от инцидентов безопасности, связанных с вредоносными программами, так что это уже не единичные инциденты. Средняя стоимость утечки данных для публичных компаний в США в 2020 году составила 116 миллионов долларов, и влияние на малые предприятия гораздо более серьезное. Например, 60% малых предприятий, ставших жертвами кибератак, прекращают свою деятельность в течение шести месяцев.

Мы думаем, что наши компании находятся в безопасном и дружелюбном месте, но как только они подключаются к Интернету, кажется, что эти предприятия находятся в захудалом районе, где бандиты за каждым углом. Тот факт, что мы не можем видеть эти риски, мешает нетехническим лидерам усвоить тот факт, что они существуют.

Правительственные учреждения и Конгресс начинают уделять внимание цифровым рискам, влияющим на общественность. Например, Colonial Pipeline, основной источник бензина и топлива для реактивных двигателей на юго-востоке США, подвергся атаке программы-вымогателя, которая остановила работу на шесть дней, что привело к нехватке газа во всем регионе поставок и затронуло миллионы зарегистрированных избирателей. Вскоре после этого инцидента Конгресс принял

Закон об отчетах о киберинцидентах для критически важной инфраструктуры от 2022 года, требующий регулирования отчетности об инцидентах в широко определенных категориях «критической инфраструктуры».

Кроме того, Комиссия по ценным бумагам и биржам (SEC) и Федеральная торговая комиссия (FTC) вступают в действие, предлагая всеобъемлющие требования к раскрытию информации о рисках и инцидентах, надлежащему использованию личной информации и ограничениям использования данных. Обширные правительственные требования заставят предприятия лучше понимать свою цифровую среду и расширят свое представление об онлайн-активности в своих организациях. Соответствие будет включать не только то, как используются данные и как отслеживается среда, но также потребует публичного раскрытия информации о соответствующих политиках и процедурах и потребует предоставления отчетов об инцидентах практически в режиме реального времени…» ***(Devin Jones. Cybersecurity Just Became a Board Issue for Real // InformationWeek (https://www.informationweek.com/security-and-risk-strategy/cybersecurity-just-became-a-board-issue-for-real). 27.09.2022).***

***

«Для протокола следует с самого начала признать, что нет никаких сомнений в том, что ландшафт кибербезопасности со временем улучшился, в основном благодаря постоянному увеличению расходов на кибербезопасность из года в год. По оценкам Gartner, в этом году США и остальной мир инвестируют в кибербезопасность 172 миллиарда долларов по сравнению со 150 миллиардами долларов в прошлом году, и в дальнейшем они будут неуклонно расти.

Эти инвестиции привели, среди прочего, к аналитике безопасности, которая представляет собой упреждающий подход к кибербезопасности, использующий возможности сбора, агрегирования и анализа данных для более эффективного обнаружения и смягчения киберугроз. Существует также растущая эффективность искусственного интеллекта и машинного обучения, и теперь архитектура с нулевым доверием вызывает интерес во многих организациях. Злоумышленникам как никогда трудно проникнуть в крупные организации.

Тем не менее, частота и масштабы кибератак продолжают расти в течение многих лет, и киберэксперты согласны с тем, что огромное количество крупных организаций уже было скомпрометировано и, вероятно, в какой-то момент снова будет скомпрометировано. Почему? Распространенным рефреном является то, что злоумышленники продолжают совершенствоваться и развиваться, и, хотя корпорации прилагают все усилия, чтобы не отставать, достаточно одного промаха, чтобы открыть дверь для киберпреступников.

Тем не менее, есть и другая важная причина, которой уделяется гораздо меньше внимания.

Многие организации по-прежнему имеют серьезные недостатки в области безопасности. К ним относятся посредственная кибер-подготовка, некачественные планы реагирования на инциденты и тенденция покупать так много инструментов безопасности, что они часто подрывают друг друга. Кроме того, согласно отчету исследовательской фирмы Lightcast, постоянно растущее количество вакансий в

сфере кибербезопасности, число которых в настоящее время только в США составляет 715 000 человек, явно недостаточно учитывается.

Есть ли решения этих недостатков? Да, но они потребуют некоторого внимания. Вот некоторые наблюдения, которые могли бы восполнить эти пробелы:

Наем на работу в области кибербезопасности нуждается в улучшении

Усугубляя нехватку кибер-работников, компании часто допускают ошибки при найме, что приводит к трудностям с подбором персонала. Все незаполненные вакансии не просто мешают предприятиям поддерживать безопасность сетей. Они также негативно сказываются на существующих командах по кибербезопасности, которые, как ожидается, будут делать все необходимое для обеспечения сетевой безопасности, используя лишь небольшую часть необходимого персонала. Это приводит к выгоранию и побуждает людей вообще уходить из отрасли.

Большая часть проблемы заключается в том, что сотрудники, которые нанимают сотрудников, не могут нарушать жесткие правила. Как и в большинстве профессий, объявления о вакансиях в области кибербезопасности сопровождаются требованиями, включая опыт и квалификацию. Как отмечается в статьях ZDNet, Protocol и других источников, отделы кадров нередко проявляют слишком строгие требования, учитывая нехватку специалистов по кибербезопасности. Некоторые из этих кандидатов профессиональны, даже не имея формальной квалификации, и тем не менее многие из них упускаются из виду при открытии вакансий.

Примером этого является то, что многим органам по сертификации кибербезопасности требуется до пяти лет доказуемого постоянного опыта работы. Эти сертификаты необходимы для многих ролей безопасности более высокого уровня. Даже кандидатам на работу со степенью в области кибербезопасности и информатики часто отказывают, потому что у них нет определенной сертификации.

Посредственная кибер-тренировка

Сотрудники обычно проходят один или два дня обучения по вопросам безопасности при приеме на работу, а затем раз в год проходят какие-то повторения. Этого недостаточно. Многие сотрудники забывают часть того, чему научились, через несколько месяцев. Несмотря на это, всем сотрудникам нужна дополнительная помощь в вопросах кибербезопасности, поскольку она постоянно меняется. Ассоциация передовых вычислительных систем рекомендует компаниям проводить тренинги по кибербезопасности каждые четыре-шесть месяцев, желательно с использованием интерактивных примеров и видео.

Важно отметить, что знания и опыт обученных сотрудников сильно различаются, что часто снижает эффективность. Некоторые исследования показали, что даже расположение сотрудников может определять вероятность того, что человек будет скомпрометирован. Одно исследование показало, что респонденты, которые идентифицировали себя как личности «типа А», не верили, что они подвергаются повышенному риску повторного использования паролей, что является рискованным занятием. Они считали, что их собственных инициативных усилий было достаточно.

Слишком много сотрудников остаются недостаточно информированными о кибербезопасности, отчасти потому, что многие руководители и менеджеры уделяют

больше внимания другим вещам, таким как накопление новых технологий для повышения производительности.

Планы реагирования на инциденты ниже номинала

Планы реагирования на инциденты предназначены для максимально быстрого реагирования на организационные нарушения, чтобы смягчить ущерб для репутации, недоверие клиентов, нормативные и судебные издержки и затраты на ликвидацию последствий. Организации должны быть устойчивыми. Исследование, проведенное IBM Security и Ponemon Institute, подчеркивает, что большинство компаний уделяют основное внимание предотвращению киберугроз, а не их устранению, и показало, что 74% специалистов по безопасности и ИТ, опрошенных на 11 мировых рынках, не считают необходимым последовательно внедрять IRP во всех своих организациях. или вообще.

Так что же делать компаниям, когда возникают серьезные проблемы с кибербезопасностью? В основном они полагаются на помощь своего отдела безопасности. Чтобы максимально смягчить утечку, гораздо больше сотрудников должны быть серьезно заинтересованы в том, чтобы быть в курсе киберугроз. Им нужно перенять избранное мышление и поведение.

Слишком много инструментов безопасности

Создание достаточного количества инструментов безопасности звучит как хорошая идея, но в основном это не так. Исследование Ponemon Institute показало, что организации в среднем используют более 45 таких инструментов. Те, кто использовал более 50, оказались на 8% ниже по способности обнаруживать атаку и на 7% ниже по способности реагировать на атаку. Проблема: все эти инструменты часто конфликтуют и подрывают друг друга.

Если решения не полностью интегрированы, что является типичным, целостное представление трудно понять, когда кибер-сотрудник перескакивает с одной компьютерной консоли на другую. Кроме того, чем больше инструментов безопасности, тем больше предупреждений (часто ложных) приходится обрабатывать. Короче говоря, сложность — это скрытая стоимость.

Руководители по информационной безопасности (CISO) считают, что необходимы еще большие инвестиции в кибербезопасность

Директора по информационной безопасности играют решающую роль в защите инвестиций в кибербезопасность, и более половины из них считают, что их советы по-прежнему не выделяют достаточно средств для снижения рисков кибербезопасности, согласно опросу, проведенному Censuswide, международной консалтинговой компанией, занимающейся исследованиями рынка. Директора по информационной безопасности говорят, что некоторые советы обсуждают кибербезопасность только во время взлома.

В этом случае сами директора по информационной безопасности являются частью проблемы. Многим нужно научиться быть более сообразительными в общении с советом директоров. Им следует избегать использования жаргона, учитывая, что правление редко состоит из киберэкспертов. Не менее важно, чтобы они не использовали страх, неуверенность и сомнения, чтобы довести до конца свою точку зрения. Они должны постоянно давать понять, что здоровье компании является наивысшим приоритетом.

Корпоративным руководителям необходимо внимательно следить за ключевыми аспектами своей инфраструктуры, такими как наличие в организации безопасной сети с защищенными пользователями и двойная проверка того, что аппаратное и программное обеспечение постоянно обновляются. Таким образом, уязвимости системы безопасности обнаруживаются раньше, чем позже.

Самое главное, лидеры должны создать культуру вокруг своей инфраструктуры безопасности. Важно, чтобы они понимали, как их руководители в настоящее время подходят к кибербезопасности и какие изменения могут потребоваться. Они должны уделять первоочередное внимание улучшению ситуации и учитывать, что еще может понадобиться в будущем. Эти шаги помогают обеспечить рост за счет цифрового доверия и укрепляют гордость сотрудников и репутацию организации среди клиентов». ***(Robert Ackerman Jr. The State of Cybersecurity has improved but is hardly flawless // Tripwire, Inc. (https://www.tripwire.com/state-of-security/security-awareness/state-of-cybersecurity-improved-but-hardly-flawless/). 25.09.2022).***

***

«Кибератаки в настоящее время настолько распространены, что большинство компаний, принявших участие в новом опросе, не только считали их главной проблемой, но и считали будущие атаки на их организации неизбежными.

В ежегодном опросе предприятий, проведенном страховым гигантом Travelers Cos., который гарантирует покрытие кибербезопасности, кибератаки были названы главной проблемой в общей среде, которая становилась все более рискованной для ведения бизнеса.

«Кибератаки могут закрыть компанию на длительный период времени или даже вывести ее из бизнеса, и крайне важно, чтобы у компаний был план смягчения любых связанных с этим операционных или финансовых сбоев», — Тим Фрэнсис, руководитель корпоративного кибербезопасности в Travelers, говорится в релизе.

Артур Хаус, бывший директор по рискам кибербезопасности в Коннектикуте, заявил в понедельник, что опрос показывает, о чем многие компании до сих пор не хотят говорить публично.

«Признание того, что вас взломали в результате кибератаки, по-прежнему вызывает клеймо, — сказал Хаус, ныне адъюнкт-профессор Университета Коннектикута, преподающий кибербезопасность. — Как будто вы не защитили себя должным образом или что-то не так. с вашими ИТ-системами».

Но Хаус сказал, что опрос указывает на то, что ни одна компания не застрахована от кибератаки.

«Это похоже на болезнь, все ею болеют», — сказал Хаус. «С вами не обязательно что-то не так».

Ключ, по словам Хауса, заключается в том, чтобы принимать как можно больше превентивных мер.

Те, кто принял участие в опросе Travelers, также заметили большую озабоченность по сравнению с прошлым годом по поводу экономической

неопределенности, роста цен на энергию и способности привлекать и удерживать сотрудников.

Опрос 1200 малых, средних и крупных компаний из 15 с лишним отраслей промышленности проводился с середины до конца июля и был проведен Hart Research for Travelers.

Путешественники начали свое исследование в 2014 году, и оно используется в качестве основы для Индекса риска путешественников. В третий раз за последние четыре года кибербезопасность стала главной проблемой для бизнеса.

Но в отличие от года назад, когда кибератаки были на 6 процентных пунктов выше следующего по величине опасения, в этом году другие проблемы были ближе к кибербезопасности.

В 2022 году 59% респондентов заявили, что они «несколько или сильно обеспокоены киберугрозами». Но за этим последовали 57%, обеспокоенные широкой экономической неопределенностью; 56% обеспокоены колебаниями цен на нефть и энергию; 56% беспокоятся о способности привлекать и удерживать таланты; и 56% обеспокоены инфляцией медицинских расходов.

Среди самых больших скачков по сравнению с прошлым годом была стоимость энергии, которая выросла на 16 процентных пунктов по сравнению с 40% год назад. Сбои в цепочке поставок увеличились на 11 процентных пунктов до 54%.

Отчет страховой компании Hiscox, опубликованный ранее в этом месяце, показал, что киберпреступники, которые долгое время преследовали крупные компании, переходят к мелким и средним работодателям.

В своем отчете Hiscox обнаружил, что компании с годовым доходом от 100 000 до 500 000 долларов теперь могут ожидать столько же кибератак, сколько и те, которые зарабатывают от 1 до 9 миллионов долларов. Тем не менее, расходы на кибербезопасность сократились у небольших фирм.

Гарет Уортон, исполнительный директор Hiscox по кибербезопасности, сказал, что пандемия, возможно, сыграла свою роль в этой тенденции.

«Переход к удаленной работе побудил многие малые предприятия принять облачные решения вместо создания собственных удаленных сервисов», — написал Уортон во введении к отчету. «Это, в свою очередь, побуждает киберпреступников использовать уязвимости в облачных приложениях, а также нацеливаться на поставщиков облачных услуг».

Атаки программ-вымогателей участились: 19% ответивших на опрос Hiscox сообщили об одной атаке в прошлом году, по сравнению с 16% годом ранее. По данным Hiscox, две трети фирм заплатили злоумышленникам.

Опрос Travelers показал, что 71% компаний, принявших участие в опросе, неоднократно становились жертвами утечки данных в результате других «киберсобытий».

«Множественные кибератаки могут быть не случайными — если вы ранее были уязвимы и в результате не предприняли соответствующих действий, вы продолжаете подвергаться риску», — сказал Фрэнсис из Travelers». ***(Kenneth R. Gosselin. Cyberattacks a top concern across all business sizes, economic uncertainty a close second, new survey shows // Tech Xplore (https://techxplore.com/news/2022-09-cyberattacks-business-sizes-economic-uncertainty.html). 27.09.2022).***

***

«Пандемия COVID-19 показала, в какой степени канадская экономика зависит от цифровой связи. В связи с недавним увеличением числа вариантов удаленной работы, предлагаемых в канадском бизнес-секторе, кибер-злоумышленники разрабатывают очень сложные методы для использования канадской цифровой инфраструктуры. В 2019 году почти 21% канадских предприятий сообщили о том, что на них повлияли инциденты кибербезопасности, число которых, по прогнозам, будет расти в Канаде в течение следующих нескольких лет. Кибер-злоумышленники часто пытаются получить деньги, потребовать выкуп или украсть личную и конфиденциальную информацию из канадских организаций. Поставщики основных услуг и критической инфраструктуры особенно подвержены риску.

Введение законопроекта C-26

14 июня 2022 года достопочтенный Марко Мендичино внес в парламент законопроект C-26, Закон о кибербезопасности, вносящий поправки в Закон о телекоммуникациях и вносящие последующие поправки в другие законы в целях борьбы с возникающими угрозами, связанными с кибербезопасностью. Законопроект C-26 вносит поправки в действующий Закон о телекоммуникациях и вводит в действие нормативную базу для кибербезопасности в соответствии с новым Законом о защите критически важных киберсистем («CCSPA»). CCSPA имеет серьезные последствия для некоторых канадских предприятий.

Назначенные операторы

CCSPA будет применяться к бизнес-операторам систем и услуг, регулируемых на федеральном уровне, которые определены в соответствии с CCSPA как «жизненно важные для национальной безопасности или общественной безопасности» («Назначенные операторы»). К назначенным операторам относятся поставщики:

телекоммуникационные услуги;

межпровинциальные или международные системы трубопроводов и линий электропередач;

ядерные энергетические системы;

транспортные системы, находящиеся в законодательной компетенции парламента;

банковские системы; а также

клиринговые и расчетные системы.

Новые обязательства

В случае принятия CCPSA уполномочит губернатора в Совете назначать назначенного оператора для защиты критической киберсистемы. Он также предоставляет некоторым регулирующим органам право входить в частную собственность, если у них есть разумные основания полагать, что в этом месте ведется какая-либо деятельность, регулируемая CCSPA, и издавать приказы о

внутреннем аудите и соблюдении требований. CCSPA также налагает следующие новые обязательства на назначенных операторов:

Программа кибербезопасности

В соответствии с CCSPA назначенные операторы будут обязаны создать и поддерживать «Программу кибербезопасности» в течение 90 дней и предоставить ее отраслевому регулирующему органу. Это влечет за собой выявление и управление рисками кибербезопасности, а также принятие мер по предотвращению компрометации киберсистем. Назначенные операторы должны будут проводить периодические проверки своих киберсистем для обеспечения их целостности.

Снижение рисков цепочки поставок и кибербезопасности

Назначенные операторы должны будут выявлять и управлять любыми киберрисками, связанными с их цепочкой поставок и использованием сторонних продуктов и услуг. Предприятия, предоставляющие аутсорсинговые услуги назначенным операторам в соответствии с CCSPA, должны знать, что их системы и методы кибербезопасности, вероятно, станут более тщательно изучаться на предмет потенциальных уязвимостей, которые могут быть использованы злоумышленниками.

Обязательные требования к отчетности

CCSPA обязывает Назначенных операторов немедленно сообщать о любом «инциденте кибербезопасности» Учреждению безопасности связи и соответствующему регулирующему органу. Инцидент кибербезопасности определяется как любое обстоятельство, которое мешает или может помешать непрерывности или безопасности жизненно важной услуги или жизненно важной системы или конфиденциальности, целостности или доступности критической киберсистемы. В отличие от действующего законодательства о конфиденциальности, инцидент кибербезопасности не обязательно должен быть связан с несанкционированным доступом к личной информации или ее раскрытием.

Раскрытие и использование информации

Обязательства, изложенные в CCSPA, также распространяются на физических лиц. С учетом определенных исключений, изложенных в CCSPA, лицо не должно сознательно раскрывать или разрешать доступ к конфиденциальной информации, которая:

касается уязвимости критической киберсистемы любого Назначенного оператора или методов, используемых для защиты этой системы;

если разумно ожидать, что раскрытие информации приведет к существенным финансовым убыткам или выгодам для Назначенного оператора, или можно разумно ожидать, что оно нанесет ущерб конкурентной позиции Назначенного оператора; или же

в случае их раскрытия можно разумно ожидать, что это помешает договорным или иным переговорам с Назначенным оператором.

Требования к ведению учета

Назначенные операторы столкнутся с повышенными требованиями к ведению учета в отношении своих киберсистем в соответствии с CCSPA. Назначенные операторы будут обязаны вести учет:

любые шаги, предпринятые для реализации программы кибербезопасности;

каждый инцидент кибербезопасности;

любые шаги, предпринятые для снижения рисков, связанных с их цепочкой поставок или сторонними продуктами и услугами; а также

любые меры, предпринятые для реализации направления кибербезопасности, данного губернатором в Совете.

Все записи, касающиеся кибербезопасности Назначенного оператора, должны храниться в Канаде в соответствии с CCSPA. Назначенные операторы должны заблаговременно определять географическое расположение серверов или центров обработки данных, где они хранят информацию, или передавать хранение или обработку такой информации на аутсорсинг, чтобы не нарушать требования CCSPA к ведению учета.

Ответственность и штрафы

Канадские предприятия должны уделять особое внимание новым обязательствам CCSPA, поскольку любое нарушение может привести к серьезному денежному штрафу. Размер штрафа будет установлен правилами, которые будут созданы в соответствии с CCSPA, и может составлять до:

1 000 000 долларов США в случае физического лица; или же

15 000 000 долларов в любом другом случае.

Директора и должностные лица Назначенного оператора могут быть привлечены к личной ответственности за нарушения в соответствии с CCSPA, если будет установлено, что они руководили, санкционировали, соглашались, молчаливо соглашались или участвовали в совершении нарушения. Должная осмотрительность может выступать в качестве защиты.

Поскольку нарушение, совершенное или продолжающееся более одного дня, считается отдельным нарушением в отношении каждого дня, в который оно было совершено или продолжалось, существует возможность применения штрафа за каждый день. Применимое наказание будет определяться с учетом характера и масштаба нарушения, усилий по смягчению последствий, истории соблюдения требований и того, была ли получена какая-либо конкурентная или экономическая выгода от нарушения. Определенные регулирующие органы уполномочены заключать соглашения о соответствии с Назначенными операторами, которые могут уменьшить штраф, подлежащий уплате.

Нарушение конкретных положений CCSPA также может быть приравнено к уголовному правонарушению, что влечет за собой лишение свободы на срок до пяти лет для физических лиц или денежный штраф для корпораций. Директор или должностное лицо Назначенного оператора, который руководил, уполномочивал, соглашался, попустительствовал или участвовал в совершении правонарушения, может быть привлечен к судебной ответственности или осужден, даже если Назначенный оператор не подвергается уголовному преследованию.

В курсе

В случае принятия законопроект C-26 послужит для федерального правительства эффективным механизмом реагирования на современные киберугрозы и повышения безопасности систем, жизненно важных для канадского общества. Положения, которые будут созданы в рамках CCSPA, будут содержать дополнительную информацию, но можно предположить, что это новое

законодательство создаст дополнительное бремя для Назначенных операторов по преодолению и увеличению рисков ответственности для директоров и должностных лиц.

Законопроект С-26 также может служить законодательной базой для принятия правительствами провинций собственного законодательства о кибербезопасности. Таким образом, все канадские предприятия должны быть в курсе изменений в канадском законодательстве о кибербезопасности, поскольку объем отраслей, к которым применяются эти новые обязательства, со временем, вероятно, расширится». ***(Jane Elise Bates. Bill C-26: New Cyber Security Obligations for Canadian Businesses Vital to National Security and Public Safety // Cox & Palmer (https://coxandpalmerlaw.com/publication/bill-c-26-new-cyber-security-obligations-for-canadian-businesses-vital-to-national-security-and-public-safety/).***

***

«Сегодня Министерство внутренней безопасности (DHS) объявило о первой в своем роде программе грантов в области кибербезопасности специально для правительств штатов, местных и территориальных (SLT) по всей стране. Эта государственная и местная программа грантов в области кибербезопасности, ставшая возможной благодаря двухпартийному закону президента Байдена об инфраструктуре, предоставляет партнерам SLT финансирование в размере 1 миллиарда долларов в течение четырех лет, из которых 185 миллионов долларов доступны на 22 финансовый год для поддержки усилий SLT по устранению киберрисков для их информационных систем. Благодаря этому финансированию правительства SLT будут лучше оснащены для устранения рисков кибербезопасности, укрепления кибербезопасности своей критически важной инфраструктуры и обеспечения устойчивости к постоянным киберугрозам для услуг, которые правительства SLT предоставляют своим сообществам.

Выпустив сегодня Уведомление о возможности финансирования (NOFO), DHS открыло процесс подачи заявок на участие в программе грантов. У соискателей есть 60 дней, чтобы подать заявку на грант, который можно использовать для финансирования новых или существующих программ кибербезопасности.

Эта программа является последним примером единого подхода DHS, в котором программа, администрируемая FEMA, использует возможности CISA для достижения цели Департамента по усилению киберзащиты на уровне штата и на местном уровне. Используя опыт управления грантами FEMA, а также опыт CISA в области кибербезопасности, DHS предпринимает шаги, чтобы помочь большему количеству заинтересованных сторон SLT по всей стране понять серьезность киберугроз и развивать партнерские отношения для снижения рисков на уровне штата, на местном уровне и на территориальном предприятии.

«Кибератаки стали одной из самых серьезных угроз для нашей родины», — сказал министр внутренней безопасности Алехандро Н. Майоркас. «В ответ мы продолжаем укреплять кибербезопасность нашей страны, в том числе путем предоставления штатам и местным сообществам ресурсов для создания и усиления их киберзащиты. Процесс предоставления грантов в области кибербезопасности, который мы начинаем сегодня, является жизненно важным шагом вперед в этом

важном начинании. Наш подход заключается в партнерстве на службе всеобщего инвестирования в безопасность нашей родины».

«По мере того, как мы строим лучшую Америку, мы обеспечиваем, чтобы наша инфраструктура была более современной и подключенной к цифровым технологиям. Но попутно мы также должны предпринимать активные шаги для повышения нашей устойчивости к растущей угрозе кибератак», — заявил координатор инфраструктуры Белого дома Митч Ландриу. «Благодаря двухпартийному закону президента об инфраструктуре мы инвестируем один миллиард долларов в кибербезопасность инфраструктуры, предоставляя нашим штатам и местным органам власти ресурсы, необходимые им для защиты от разрушительных киберугроз. Сегодняшнее объявление знаменует собой важный шаг в нашем стремлении повысить устойчивость, защитить и улучшить инфраструктуру нашей страны и защитить нашу экономику».

«Как национальное агентство по киберзащите, CISA работает рука об руку с нашими партнерами в государственных, местных и территориальных органах власти, которые сталкиваются с уникальными проблемами кибербезопасности, но часто не имеют ресурсов для их решения. Государственная и местная программа грантов в области кибербезопасности сыграет решающую роль в оказании помощи этим организациям в наращивании их возможностей и потенциала», — сказала директор CISA Джен Истерли. «Мы призываем все правомочные организации подавать заявки на получение грантов для защиты нашей критически важной инфраструктуры и сообществ от злонамеренной киберактивности и расширения их партнерства с CISA. CISA готова предоставить экспертные знания, инструменты и техническую помощь, чтобы стать надежным партнером правительств штатов, местных и территориальных органов власти в борьбе с растущими киберугрозами, с которыми они сталкиваются каждый день».

«Миссия FEMA по оказанию помощи людям до, во время и после стихийных бедствий не ограничивается событиями, связанными с климатом. Реагирование на техногенные угрозы критически важной инфраструктуре нашей страны, такой как кибербезопасность, — это роль, к которой мы относимся серьезно и готовы поддержать», — сказала администратор FEMA Дин Крисвелл. «Мы ценим наше партнерство с CISA и с нетерпением ждем возможности управлять этой новой программой грантов в области кибербезопасности, которая поможет защитить важные ресурсы по всей стране и обеспечит, чтобы правительства штатов, местных и территориальных властей имели больше инструментов, чтобы стать более устойчивыми ко всем опасностям».

«Сегодняшнее заявление является еще одним примером приверженности президента Байдена обеспечению основных услуг, на которые полагаются американцы. Администрация Байдена-Харриса стремится пробовать новые творческие подходы, такие как эта программа грантов для правительств штатов и местных органов власти, для усиления нашей киберзащиты для защиты американцев, которым мы служим», — сказала Энн Нойбергер, заместитель советника по национальной безопасности по вопросам кибербезопасности и новых технологий.

«Для обеспечения безопасности национальной киберэкосистемы требуется подход с участием всего общества, который включает в себя важнейшую работу, которую правительства штатов, местные и территориальные органы ежедневно выполняют в партнерстве с федеральным правительством. Эта программа, ставшая возможной благодаря двухпартийному закону об инфраструктуре, демонстрирует приверженность администрации Байдена-Харриса обеспечению того, чтобы все американцы могли процветать в киберпространстве», — сказал национальный директор по кибербезопасности Крис Инглис.

Программа кибергрантов — это инновационная программа, созданная в соответствии с Законом об улучшении кибербезопасности на уровне штатов и на местном уровне, который является частью Закона о двухпартийной инфраструктуре, чтобы помочь решить уникальные проблемы, с которыми сталкиваются правительства штатов и территорий при защите от киберугроз. Эта новая программа грантов поможет государственным и местным партнерам снизить киберриски и повысить устойчивость к динамичной и развивающейся среде угроз кибербезопасности.

В частности, программа кибергрантов будет финансировать усилия по созданию критически важных структур управления в штатах и территориях для устранения киберугроз и уязвимостей, выявления ключевых уязвимостей и оценки необходимых возможностей, реализации мер по смягчению угроз и развития кибер-трудовых ресурсов 21-го века по всему миру. местные сообщества. CISA будет поддерживать эти усилия с помощью набора доступных ресурсов, включая государственных координаторов по кибербезопасности и советников по кибербезопасности.

Гранты значительно повысят национальную устойчивость к киберугрозам, предоставив правительствам штатов, местных и территориальных органов столь необходимые ресурсы для решения проблем сетевой безопасности и принятия мер по защите от рисков кибербезопасности, чтобы помочь им укрепить свои сообщества. Для этой программы будет две возможности финансирования. Объявленная сегодня возможность финансирования предназначена для государственных, местных и территориальных органов власти. В рамках этого NOFO местные органы власти являются правомочными субреципиентами через свои соответствующие штаты и территории. Отдельная программа племенных грантов будет выпущена позже осенью». ***(Biden-Harris Administration Announces $1 Billion in Funding for First-Ever State and Local Cybersecurity Grant Program // DHS.gov (https://www.dhs.gov/news/2022/09/16/biden-harris-administration-announces-1-billion-funding-first-ever-state-and-local). 16.09.2022).***

***

«Наступил еще один месяц осведомленности о кибербезопасности. По данным Национального альянса кибербезопасности (NCA), мы отмечаем это событие уже восемнадцатый год. 18 лет назад мы увидели запуск Facebook, Gmail, MySpace, Roblox, IPO Google и вирус MyDoom. Перенесемся в 2022 год, когда атаки и уязвимости теперь появляются на первых страницах, казалось бы, ежедневно, кибербезопасность важнее, чем когда-либо.

Что такое Месяц осведомленности о кибербезопасности?

Месяц осведомленности о кибербезопасности, запущенный в 2004 году под руководством Министерства внутренней безопасности США и NCA, направлен на то, чтобы помочь американцам оставаться в безопасности в Интернете. С тех пор движение росло в геометрической прогрессии, повышая осведомленность потребителей, малого и среднего бизнеса (SMB), предприятий и образовательных учреждений.

Месяц осведомленности о кибербезопасности имеет смысл

Главной темой на 2022 год является «Увидь себя в киберпространстве», в которой основное внимание уделяется четырем ключевым моделям поведения, а не еженедельным темам, основанным на подходе, основанном на оценке рисков. Это поведение:

Включение многофакторной аутентификации (MFA)

Использование надежных паролей и менеджера паролей

Обновление программного обеспечения

Распознавание фишинга и сообщение о нем

Это, безусловно, отличное место для начала, но компании любого размера должны стремиться сделать все возможное, чтобы улучшить свою кибербезопасность. Вот три дополнительных действия, которые любая организация может предпринять, чтобы продемонстрировать улучшение:

Уменьшите неизвестную поверхность атаки

Полагаться на базы данных управления вашей ИТ-системой недостаточно точно. Знайте, что происходит в вашей сети: законные, теневые ИТ или подключенные через VPN, получайте более точную инвентаризацию. Злоумышленники знают, что устройства, которые не управляются и/или не исправлены, являются лучшими боковыми путями.

Знайте, что для получения наилучшей картины необходимы как внешнее управление поверхностью атаки (EASM), так и внутреннее управление поверхностью атаки киберактивов (CAASM). Видимость является основой всех других средств защиты.

Полугодовые тесты на проникновение ставят галочку и защищают вас от тюрьмы соответствия, но кибербезопасность перешла к почти реальному времени, и ваша оценка тоже должна быть. Непрерывный мониторинг был важной целью, но нам необходимо продвигать его к принятию непрерывных решений на основе этого непрерывного мониторинга.

Даже такие события, как аутентификация для использования VPN, слишком редки, чтобы делать обоснованные суждения: между этими аутентификациями может быть много индикаторов компрометации (IOC), которые дают достаточно высокую уверенность в том, что вы или ваша учетная запись/устройство/актив/данные были перемещены. от приемлемого до неприемлемого риска.

Непрерывная оценка означает постоянный поиск уязвимых или скомпрометированных элементов и принятие мер. Если мое устройство уязвимо, или моя учетная запись электронной почты извергает вредоносное ПО, или признаки

фишинга, должно быть принято немедленное решение, основанное на оценке риска. Время — друг нападающего. Давайте будем менее дружелюбными с ними.

Увеличьте нестандартную телеметрию безопасности

Стандартные события, которые мы изучаем в области безопасности, не только немного устарели, но и злоумышленники знают их достаточно хорошо, чтобы не попасться на них. Это вся основа для атак, которые могут перемещаться в боковом направлении и по нетрадиционным путям, таким как Интернет вещей и вещи, о которых, вероятно, не известно, что они являются частью вашей поверхности атаки, когда они есть.

Злоумышленники знают, где находятся датчики движения для стандартных предупреждений безопасности и телеметрии, и избегают их. Помимо того, что вы лучше знаете свою поверхность атаки, идите и собирайте больше новых видов телеметрии, связанных с безопасностью.

Расширенное обнаружение и реагирование (XDR) и непрерывная оценка становятся умнее, быстрее и точнее, когда есть больше данных для оценки, помимо предупреждений брандмауэра ваших родителей. Телеметрия, касающаяся подключений, количество пропущенных аутентификаций, изменения в активности приложений, использование DNS, системные инструменты, работающие в новых местах, невиданные ранее пары привилегий и предоставление администратора, необычные резервные копии… есть озеро данных, чтобы заполнить их. Чем больше у вас телеметрии, тем больше вы можете комбинировать их в более значимые индикаторы, которые с меньшей вероятностью будут ложноположительными или ложноотрицательными.

Выбор правильных инструментов безопасности

Подчеркивая все это, вам нужны правильные инструменты безопасности. Хотя вы можете диверсифицировать свой стек безопасности, не попадитесь в ловушку развертывания точечных продуктов, которые плохо сочетаются друг с другом. Как я уже сказал, видимость — это основа всех других средств защиты. Использование разрозненных решений даст вам только фрагменты полной картины.

Вам не нужно разрывать и заменять весь стек — это дорого и требует много времени. Однако вы можете использовать унифицированную платформу кибербезопасности, которая объединяет телеметрию из разных решений безопасности в единую панель. Будьте осторожны, некоторые поставщики могут попытаться продать вам набор разрозненных решений в качестве платформы. Настоящая платформа состоит из интегрированных решений поставщиков и допускает широкую интеграцию сторонних производителей.

В качестве бонуса ищите платформу, которая поддерживает возможности, о которых я упоминал ранее, такие как XDR, виртуальное исправление, автоматизация, непрерывный мониторинг и многое другое, чтобы обеспечить безопасность на всей поверхности атаки — от пользователей до конечных точек, электронной почты, облаков и т. д. сети и т.д.

Итак, давайте сделаем Месяц осведомленности о кибербезопасности действенным и содержательным. И в духе постоянной оценки не ждите следующего Месяца осведомленности о кибербезопасности, чтобы проверить и уточнить свой прогресс…» ***(Greg Young. Cybersecurity Awareness Month 2022: 3 Actionable Tips //***

Trend Micro Incorporated (https://www.trendmicro.com/en_us/ciso/22/i/cybersecurity-awareness-month-3-actionable-tips.html). 20.09.2022).

***

«Новое исследование показало, что многие штаты и округа стали жертвами киберугроз или атак, но немногие государственные чиновники считают, что их правительство реагирует должным образом.

Согласно недавно опубликованному отчету State EdTech Trends за 2022 год, 70 процентов из 80 опрошенных государственных чиновников говорят, что либо их государственное образовательное учреждение, либо по крайней мере один школьный округ подверглись кибератаке или угрозе в прошлом году.

Но только 6% респондентов говорят, что их штат выделяет достаточно средств на кибербезопасность.

Отчет, выпущенный некоммерческой ассоциацией директоров по образовательным технологиям штата в сотрудничестве с Whiteboard Advisors, направлен на отслеживание того, как государственные образовательные учреждения адаптируются к технологиям и образованию после пандемии.

Более половины респондентов, в число которых входят члены SETDA, суперинтенданты штатов и другие высокопоставленные государственные чиновники из всех 50 штатов, говорят, что в их штате существуют общегосударственные инициативы, связанные с широкополосной связью (59 процентов), кибербезопасностью (54 процента) и технологиями для обучение (53%).

Но также выяснилось, что штаты не имеют последовательных определений или категорий для образовательных технологий. И многие респонденты сообщают о несоответствии между их приоритетами в области образования и инвестициями государства в образовательные технологии, которые могли бы поддержать эти приоритеты.

«Это буквально 50 разных штатов», — сказала исполнительный директор SETDA Джули Фэллон, подчеркнув разнообразие.

Согласно отчету SETDA, менее половины респондентов, 48 процентов, говорят, что их государственное агентство по образованию открыто говорит о роли технологий в поддержке государственных приоритетов.

И только 41% говорят, что люди, работающие над технологиями образования на государственном уровне, регулярно участвуют в более широком планировании и стратегических обсуждениях технологий.

Отсутствие координации по Ed Tech

Частично это объясняется большим разнообразием подходов штатов к образовательным технологиям. Чуть более половины государственных образовательных агентств, 55 процентов, имеют специальный офис, который координирует образовательные технологии, а те, которые действительно имеют различные должности, руководство и структуру для этих офисов.

В большинстве штатов над программами в области образовательных технологий работают от двух до пяти сотрудников, но исследование показало, что только 27% респондентов говорят, что лицо, отвечающее за технологии в сфере образования, регулярно встречается с главой штата.

По словам Фэллон, если опыт в области технологий не будет включен в штат государственных органов, прогресс может прерываться новым руководством каждые четыре года, и эти сотрудники должны быть осведомлены о подходе государства к совершенствованию технологий и о том, как оно поддерживает государственные приоритеты.

«Определение роли образовательных технологий в ЮВА будет особенно важно, поскольку государства продолжают адаптироваться к все более цифровому постпандемическому миру», — говорится в отчете.

Забегая вперед, Фэллон сказал, что директора по технологиям образования штатов будут думать о том, как сохранить некоторые инвестиции, сделанные их штатами во время пандемии. Один из способов сделать это — попытаться собрать более достоверные доказательства эффективности продуктов.

Цель состоит в том, чтобы показать, что финансирование принесет долгосрочные выгоды и было больше, чем «одноразовый выстрел», сказала она.

Другие ключевые выводы из отчета:

Пятьдесят семь процентов респондентов говорят, что в их штатах есть много образовательных программ и продуктов, но они не всегда используют их эффективно.

Восемь штатов собирают как минимум некоторые данные как об использовании, так и об эффективности инструментов образовательных технологий. Пока 19 штатов не собирают данные по этому поводу.

Подавляющее большинство респондентов (74 процента) говорят, что главными приоритетами в области образования в их штатах являются набор и удержание преподавателей, а также решение проблем с отставанием в обучении (72 процента)». ***(Emma Kate Fittes. Few State Officials Believe Their Cybersecurity Funding Is Keeping Up With Threats // Editorial Projects in Education, Inc. (https://marketbrief.edweek.org/marketplace-k-12/state-officials-believe-cybersecurity-funding-keeping-threats/). 15.09.2022).***

***

«Управление по контролю за иностранными активами Министерства финансов добавляет новые общие лицензии к правилам, которые определяют, выносят ли они санкции за подрыв кибербезопасности.

«OFAC добавляет в правила три новые общие лицензии: общую лицензию, разрешающую инвестирование и реинвестирование определенных средств… общую лицензию, разрешающую официальную деятельность правительства США… и общую лицензию, разрешающую определенную официальную деятельность международных субъектов и организаций, — говорится в уведомлении, опубликованном во вторник в Федеральном реестре.

Правила были впервые опубликованы во исполнение указа президента Барака Обамы от апреля 2015 года об утверждении санкций за злонамеренную кибератаку. Они переиздаются для учета последующих соответствующих приказов и законов, касающихся угроз кибербезопасности со стороны иностранных противников, включая Россию.

В первоначальном исполнительном указе Китай конкретно не упоминается, но он был предшественником соглашения между Обамой и китайским лидером Си Цзиньпином о том, какие виды кибератаки — например, кража интеллектуальной собственности — должны быть запрещены. В 2020 году президент Дональд Трамп воспользовался теми же чрезвычайными полномочиями, чтобы издать Указ № 13959: «Устранение угрозы со стороны инвестиций в ценные бумаги, которые финансируют коммунистические китайские военные компании».

Обновленные правила, которые включают в себя ключевые определения — например, для таких терминов, как «значительная деятельность, подрывающая кибербезопасность», — появляются, когда исполнительная власть снова стремится показаться жесткой по отношению к Китаю. США недавно запретили производителю чипов NVIDIA экспортировать туда товары — за исключением специальной лицензии — и, как сообщается, администрация рассматривает другие соответствующие исполнительные указы, в том числе приказ, который сократит инвестиции США в китайские компании.

Согласно уведомлению Федерального реестра, правила будут применяться к применению санкций в соответствии с текущей политикой США, «а также к санкциям, которые могут быть изложены в любых будущих исполнительных указах, изданных в связи с чрезвычайным положением в стране, объявленным в ЕО 13694». ***(Mariam Baksh. Treasury Reissues Rules to Enforce Cyber Sanctions on Foreign Adversaries // Nextgov (https://www.nextgov.com/cybersecurity/2022/09/treasury-reissues-rules-enforce-cyber-sanctions-foreign-adversaries/376783/). 06.09.2022).***

***

«Окончательная версия практики кибербезопасности Национальной администрации безопасности дорожного движения будет опубликована в Федеральном реестре в пятницу, в ней основное внимание будет уделено криптографическим методам для снижения рисков взлома по мере того, как транспортные средства становятся более технологически интегрированными.

В окончательном варианте передового опыта кибербезопасности для обеспечения безопасности современных транспортных средств официальные лица НАБДД воспользовались советами общественности во время периода открытого обсуждения проекта публикации и добавили более подробную информацию о ключевых системах и криптографических элементах, а также о том, как злоумышленники могут использовать обновления программного обеспечения для проникновения. сеть автомобиля.

Другие темы, которые были добавлены в объем руководства в соответствии с общественными комментариями, включают вопросы права на ремонт, новые ссылки на исходные материалы и изменение формулировок.

«Рекомендации, содержащиеся в передовой практике, предназначены для применения ко всем лицам и организациям, участвующим в проектировании, разработке, производстве и сборке автомобиля, его электронных систем и программного обеспечения», — говорится в уведомлении Федерального реестра.

Объекты, на которые распространяются рекомендации, включают в себя как малые, так и большие автомобили, а также предназначены для использования

разработчиками и производителями автомобильного оборудования. Каждое руководство направлено на предотвращение ответственности, связанной с внедрением новых технологий в современные автомобили.

Авторы отчета NHTSA, в частности, признали отсутствие обширных знаний в области автомобильной кибербезопасности, поскольку эта область все еще развивается. Учитывая разнообразие организационной структуры автомобильной промышленности, официальные лица отметили, что разные поставщики и производители имеют разные уровни угроз кибербезопасности.

Несмотря на это, официальные лица рекомендовали соответствующим компаниям и заинтересованным сторонам принять надлежащие меры безопасности.

«Что касается преимуществ, организации, которые не применяют надлежащие меры кибербезопасности, такие как те, которые руководствуются этими рекомендациями или другими надежными средствами контроля, сталкиваются с более высоким риском кибератаки или повышенным риском в случае кибератаки, что может привести к проблемам безопасности для населения, — говорилось в уведомлении.

Первые рекомендации NHTSA по кибербезопасности для автомобильных транспортных средств были выпущены в 2016 году. Обновленные рекомендации отражают изменения в автомобильной промышленности, а именно усиление интеграции автомобильных операций с доступом к Интернету вещей». ***(Alexandra Kelley. Traffic Safety Agency Issues Final Guidelines for Vehicle Cybersecurity // Nextgov (https://www.nextgov.com/cybersecurity/2022/09/traffic-safety-agency-issues-final-guidelines-vehicle-cybersecurity/376890/). 08.09.2022).***

***

«Агентство кибербезопасности и безопасности инфраструктуры использует самую широкую сеть, чтобы получить отзывы о реализации Закона об отчетности о кибер-инцидентах для критически важной инфраструктуры, прося заинтересованных сторон высказать свое мнение о самых основных терминах, используемых в законодательстве.

В запросе на информацию, опубликованном в Федеральном реестре в понедельник, CISA объявила о серии слушаний, которые она планирует провести по всей стране до середины ноября, чтобы проинформировать о правиле, которое она должна издать для обеспечения соблюдения закона, принятого Конгрессом в марте после нескольких высокопоставленных профилировать нарушения кибербезопасности у поставщиков критически важной инфраструктуры.

Среди них была атака на Colonial Pipeline, за обезвреживание которой компания заплатила многомиллионный выкуп. Помимо сообщения о «закрытых киберинцидентах» в CISA в течение не менее 72 часов, закон требовал, чтобы «подпадающие под действие организации» сообщали агентству о любых «выплатах выкупа» в течение 24 часов.

В соответствии с этими и другими критериями закон оставляет на усмотрение CISA определение того, что считается «охватываемым объектом» и «охватываемым инцидентом кибербезопасности» в следующем правиле.

«Термин «охватываемый кибер-инцидент» означает существенный кибер-инцидент, с которым столкнулась застрахованная организация, который удовлетворяет определению и критериям, установленным директором [CISA] в окончательном правиле», — говорится, например, в нем.

С этой целью в отчете CISA RFI респондентам предлагается указать, помимо прочего, «значение термина «существенный кибер-инцидент». частота, с которой злоумышленники постоянно пытаются проникнуть в критическую инфраструктуру с разным уровнем успеха. Как регулярно отмечает директор CISA Джен Истерли, это было бы излишне обременительным как для представителей отрасли, так и для государственных чиновников, направляющих отчеты в агентство.

Но RFI также запрашивает отзыв о значении терминов «выкуп» и «атака программ-вымогателей», которые уже полностью определены законодательством, наряду с «компрометацией цепочки поставок».

CISA также запрашивает информацию о «критериях для определения того, является ли организация многосторонней организацией, которая разрабатывает, внедряет и обеспечивает соблюдение политик, касающихся системы доменных имен». В законе отмечается, что его не следует применять против таких организаций, как Интернет-корпорация по присвоению имен и номеров или Управление по присвоению номеров в Интернете.

В дополнение к общественному мнению, нормотворчество CISA также должно быть проинформировано другими федеральными агентствами, ряд из которых могут иметь противоречивые требования к организациям, находящимся в их конкретной юрисдикции, сообщать о соответствующих инцидентах кибербезопасности.

CISA также планирует прослушивание в Вашингтоне, округ Колумбия, а также прослушивание в конкретных секторах. Но, согласно уведомлению Федерального реестра, детали этих сессий еще не определены. В пятничном пресс-релизе агентство заявило, что оно также примет письменные комментарии по нормотворчеству в течение следующих 60 дней». ***(Mariam Baksh. CISA Requests Input on Terms Already Defined by Incident Reporting Law // Nextgov (https://www.nextgov.com/cybersecurity/2022/09/cisa-requests-input-terms-already-defined-incident-reporting-law/377023/). 12.09.2022).***

***

«Команда национального директора по кибербезопасности Криса Инглиса работает над планом решения проблемы нехватки специалистов по кибербезопасности и повышения осведомленности и образования в области кибербезопасности.

Ни для кого не секрет, что в кибериндустрии не хватает талантов. По последним оценкам, количество вакансий превышает 714 000, согласно CyberSeek, проекту, поддерживаемому Национальным институтом стандартов и технологий.

В правительстве различные агентства и ведомства использовали различные инструменты, стратегии и программы, чтобы попытаться расширить кадровый резерв и заполнить рабочие места — ситуация, которая побудила две экспертные группы рекомендовать в двух отдельных отчетах в этом году, что Inglis координирует свои усилия и секторы.

Теперь Управление национального директора по кибербезопасности начинает работу над национальной стратегией в области кибербезопасности и образования, о которой было объявлено на саммите по кибербезопасности этим летом.

Вопрос рабочей силы является одним из его главных приоритетов, сказал Инглис вчера на мероприятии, организованном Billington Cybersecurity. Его офис в настоящее время ищет найма кого-то, кто конкретно занимается вопросами рабочей силы.

В пространстве федерального правительства предстоящая стратегия прояснит роли между различными государственными субъектами и определит показатели для измерения проблемы и того, насколько хорошо работают усилия по ее решению, заявила Камилла Стюарт Глостер, заместитель национального кибер-директора по технологиям и безопасности экосистемы…

«Есть некоторые вещи, которые нужно изменить. Есть некоторые программы, которые нужно расширять. Есть некоторые, которые, возможно, придется сократить. Вы должны увидеть некоторые изменения в ближайшие годы в результате этой стратегии и инфраструктуры, которую мы создадим для стимулирования реализации», — сказала она. «Цель состоит в том, чтобы создать механизм реализации и слаженность посредством сотрудничества и постоянного диалога на уровне руководства, которые должны фактически способствовать достижению целей, которые мы обозначили в нашей стратегии», — продолжила она». ***(Natalie Alms. A Cyber Workforce Strategy is Coming From the White House, Along with an Implementation Body to Make Sure it Works // Nextgov (https://www.nextgov.com/cybersecurity/2022/09/cyber-workforce-strategy-coming-white-house-along-implementation-body-make-sure-it-works/377030/). 12.09.2022).***

***

«Исследователи из ThriveDX объявили сегодня о заметном росте использования программ повышения осведомленности о кибербезопасности во всех отраслях за последний год, что привело к повышению уровня безопасности на большинстве предприятий. Полученные результаты являются частью недавно опубликованного Глобального учебного исследования по повышению осведомленности о кибербезопасности 2022 года, в котором приняли участие более 1900 директоров по информационной безопасности, руководителей в области безопасности и ИТ-специалистов.

Почти все опрошенные организации, в общей сложности 97%, сообщили о том, что в прошлом году применяли те или иные меры по повышению осведомленности о кибербезопасности, при этом большинство из них в настоящее время используют комбинацию как моделирования фишинга, так и обучения по повышению осведомленности о безопасности. Однако из 1900 опрошенных специалистов по безопасности только 42% сообщили о привлечении своих сотрудников к обнаружению безопасности с использованием таких мер, как кнопка обнаружения фишинга. Это важное отличие, поскольку известно, что этот тип взаимодействия способствует повышению безопасности за счет создания виртуального «человеческого брандмауэра» и ускорения сообщения о потенциальных угрозах.

«Эта статистика говорит нам о двух вещах. Во-первых, осведомленность о кибербезопасности в настоящее время достигает подросткового возраста, и почти все согласны с тем, что регулярное обучение повышает безопасность предприятия так, как это не могут сделать одни только технологии», — сказал Аарон Бостик, директор по информационной безопасности ThriveDX в Северной Америке. «Во-вторых, эти цифры показывают нам, что нам еще предстоит пройти долгий путь, чтобы достичь зрелости и понимания того, что единственный верный способ снизить современные киберриски — это позитивно изменить поведение сотрудников и создать позитивную культуру безопасности в наших компаниях».

65% опрошенных ИТ-специалистов согласились с тем, что их учебные программы по повышению осведомленности о кибербезопасности нуждаются в расширении, и никто не выразил желания сократить свое текущее участие.

Результаты усилий по повышению осведомленности сотрудников были впечатляющими по всем направлениям: 19% сообщили о повышении осведомленности; на 14% больше бдительности; 12% заявили, что усилили свой человеческий брандмауэр; и 99% сообщают об увеличении корпоративной безопасности. 96% также отметили положительное влияние на общую рабочую атмосферу на их предприятии. Участники опроса сообщили, что наиболее важными факторами успеха являются продолжительность курса обучения, развлекательный характер, персонализация и индивидуализация.

«Это действительно подтверждает ориентированный на человека подход, который мы применяем к обеспечению безопасности», — сказал Рой Зур, генеральный директор ThriveDX for Enterprise. «Вовлечение сотрудников, предложение индивидуального обучения по вопросам безопасности и обеспечение их приверженности безопасности — это способ номер один снизить киберриски».

Другие ключевые выводы:

В настоящее время наиболее популярными темами обучения являются курсы по фишингу и вредоносным программам, безопасности паролей, безопасности электронной почты, социальной инженерии и программам-вымогателям.

72% воздерживаются от предварительного оповещения сотрудников о фишинговых кампаниях

Самыми большими проблемами, связанными с внедрением программ повышения осведомленности, были достижение одобрения пользователей (25%), рабочая нагрузка и ресурсы (22%) и выполнение программы (14%).

Использование заявлений о целях, политик, руководств, показателей и систематического обучения растет: 58% респондентов сообщили о том, что в той или иной форме действуют правила обеспечения безопасности». ***(Study Shows Increased Maturity in Cybersecurity Awareness Programs and Higher Level of Security at Most Companies // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/study-shows-increased-maturity-in-cybersecurity-awareness-programs-and-higher-level-of-security-at-most-companies/). 06.09.2022).***

***

«Счетная палата правительства (GAO) заявляет, что федеральному правительству необходимо разработать и реализовать комплексную стратегию по преодолению киберугроз, с которыми сталкиваются Соединенные Штаты.

В последние годы Федеральное бюро расследований (ФБР) стало свидетелем того, как китайские хакеры, спонсируемые государством, неустанно ищут способы компрометации неисправленных сетевых устройств и инфраструктуры.

В июне этого года ФБР объявило, что китайские хакеры, спонсируемые государством, атаковали крупные телекоммуникационные компании и поставщиков сетевых услуг и взламывали их, по крайней мере, с 2020 года. и фармацевтическом секторах для компрометации учетных записей Microsoft Office 365 и Outlook. В апреле Соединенные Штаты удалили российское вредоносное ПО из компьютерных сетей по всему миру, а платформа социальных сетей предотвратила две кампании кибершпионажа, связанные с Ираном, которые были нацелены на активистов, ученых и частные компании в странах, включая США, с использованием фишинга и других методов социальной инженерии. методы. Управление по контролю за иностранными активами Министерства финансов США приписало взлом сети Ronin Network в марте 2022 года северокорейской хакерской группе и объявило санкции против хакеров.

Это всего лишь несколько примеров недавних нападений со стороны национальных государств. США также должны противостоять атакам киберпреступников. Заместитель помощника министра обороны по киберполитике заявил в мае, что преступные хакеры также могут действовать разрушительным образом и сильно влиять на американский образ жизни, как, например, в случае атаки прошлым летом на Colonial Pipeline.

«Разграничение между хакером-преступником и хакером национального государства усложняет защиту нации», — сказал Мике Эоян. «Проблему еще больше усложняет то, что некоторые страны, хотя они, возможно, никогда напрямую не совершали кибератаки на США, делают себя гостеприимными для хакеров-преступников, которые заинтересованы в получении выгоды от таких атак».

Ранее, в сентябре 2020 года, GAO сообщило, что Национальная киберстратегия предыдущей администрации на 2018 год и связанный с ней План реализации на 2019 год касались некоторых, но не всех желаемых характеристик национальных стратегий. GAO рекомендовало Совету национальной безопасности работать с соответствующими федеральными органами для обновления документов по стратегии кибербезопасности.

В 2021 году Конгресс учредил Управление национального директора по кибербезопасности, чтобы возглавить национальные усилия по кибербезопасности. Офис был создан для преодоления проблем, связанных с киберпространством, таких как деятели национального государства и преступники, крадущие личную информацию американцев с помощью социальной инженерии в киберпространстве. С июня 2021 года директор разработал стратегическое заявление для Управления и нанял сотрудников.

По состоянию на август 2022 года Управление сообщило, что в нем работает около 55 сотрудников, а к концу 2022 финансового года их число может вырасти примерно до 75 сотрудников. Одним из ключевых назначений директора был

заместитель национального кибер-директора по федеральной кибербезопасности, который также работает в Административно-бюджетное управление в качестве федерального главного сотрудника по информационной безопасности. По словам директора, двойная роль предназначена для предоставления экспертных знаний по вопросам бюджета и кибербезопасности в рамках Управления.

По данным Управления, по состоянию на август 2022 года администрация активно разрабатывает национальную стратегию кибербезопасности. Управление сообщило GAO, что оно получает отзывы о стратегии от многих других федеральных органов, включая Совет национальной безопасности, в отношении этих усилий». ***(Kylie Bielby. GAO: Comprehensive Strategy Needed to Overcome Cyber Threats // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/gao-comprehensive-strategy-needed-to-overcome-cyber-threats/). 08.09.2022).***

***

«По мере роста зависимости мира от технологий растет и потребность в кибербезопасности. Сорок четыре процента предприятий обеспокоены растущей угрозой кибератак на их данные и информацию. Пандемия сделала рабочее место более цифровым, чем когда-либо прежде, предоставив хакерам прекрасную возможность взломать данные и украсть личную информацию. Только с 2019 по 2020 год в США число жертв кибербезопасности и кражи личных данных увеличилось на 311 процентов.

Кроме того, законодательство о кибербезопасности также находится в разработке: президент Байден подписал двухпартийный Закон об отчетности о кибер-инцидентах в марте этого года, поскольку глобальные компании сталкиваются с повышенными рисками из-за угроз программ-вымогателей и опасений кибератак со стороны России после ее вторжения в Украину. Критическая инфраструктура, такая как больницы, электростанции и топливопроводы, особенно уязвима для хакеров и подобных атак.

Однако по мере роста этих опасений предприятия и сотрудники принимают вызов и применяют упреждающий подход для защиты себя и данных своей компании от различных угроз и атак, в том числе уделяя больше внимания планированию кибербезопасности в своих исполнительных командах, интеграции целостного инцидента. планы реагирования и внедрение новых технологий. Ниже приведены три тенденции кибербезопасности, которые положительно влияют на эту область.

Развитие управления кибербезопасностью в организации

Внутренняя реструктуризация управления кибербезопасностью — это огромный сдвиг, происходящий во многих организациях по мере развития и усложнения атак. Традиционно корпоративные компании нанимают главного сотрудника по информационной безопасности (CISO) для оценки угроз и реагирования на них, а главный исполнительный директор (CEO) и совет директоров играют второстепенную роль в планировании и защите кибербезопасности. В будущем ответственность за кибербезопасность внутри корпорации будет распределена между многими руководителями. Роль директора по информационной

безопасности изменится на эксперта в предметной области, который будет оценивать ландшафт угроз и фактические риски, определять затраты, связанные со страхованием кибербезопасности и защитными решениями, а также рекомендовать комплексный план реагирования на инциденты. Вооружившись этой информацией, затем генеральный директор или совет директоров примут ответные решения и будут действовать в соответствии с этими рекомендациями. Точно так же готовность и планирование кибербезопасности станут ключевыми критериями при оценке руководителей, и советы директоров также будут привлекать их к ответственности, если организация окажется неподготовленной.

Создание корпоративной группы реагирования на инциденты

Основная цель любого умного реагирования на безопасность — предотвращение. Комплексный подход к безопасности и оценке рисков является стандартным вопросом, когда речь идет о физической безопасности, но все больше и больше компаний осознают важность защиты своих цифровых данных, а также персонала. В рамках этого признания компании, которые ранее не имели центра управления безопасностью (SOC) или превентивных мер, предпринимают активные шаги по созданию плана реагирования на инциденты, оценивая имеющиеся у них меры предосторожности, если таковые имеются, и сравнивая их с нормативные требования. Эти оценки, часто продиктованные бизнес-моделью организации, представляют собой дорожную карту четких шагов по повышению безопасности.

Эти исследования и разработки приводят к созданию и внедрению плана и команды реагирования на инциденты, поскольку цель всегда состоит в том, чтобы предотвратить возникновение и распространение угрозы. Эти планы реагирования содержат четкие и действенные шаги, которым должны следовать сотрудники, чтобы защитить, предотвратить, проанализировать и отреагировать на угрозу кибербезопасности, и включают целостный подход к кибербезопасности, от покупки продукта, установки и развертывания до круглосуточного мониторинга. и управление всеми цифровыми каналами компании.

Использование новых технологий

Индустрия кибербезопасности развивалась благодаря технологическим достижениям, особенно за последние 20 лет. Однако для борьбы с растущим числом и сложностью потенциальных угроз требуется гораздо больший рост и развитие. Постоянно проводятся исследования, разработки и инновации для разработки решений по мере появления новых угроз. Сообществу в целом не хватает информации о потенциальных угрозах, что является общей тенденцией в области безопасности. Данные, предоставляемые защитой конечных точек, защитой от угроз электронной почты, брандмауэрами, унифицированными платформами управления угрозами и системами предотвращения вторжений и всесторонне обрабатываемые через SOC, обеспечивают более эффективный метод защиты цифровых активов компании и более быстрое и разумное реагирование на угрозы.

Несмотря на рост угроз, будущее кибербезопасности выглядит радужным. В целом компании и их сотрудники стали более усердными и понимают важность защиты своих цифровых активов. Перераспределение ответственности за кибербезопасность внутри корпоративных исполнительных команд, разработка целостных планов реагирования на инциденты и внедрение новых технологий — все

это способствует улучшению перспектив. По мере того, как все больше компаний начинают обращать внимание и понимать эти угрозы и важность мер предосторожности, ландшафт кибербезопасности будет продолжать набирать обороты и улучшаться». ***(David Rickard. The Future of Cybersecurity // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/the-future-of-cybersecurity/). 15.09.2022).***

***

«Министерство юстиции США объявило в конце прошлого года, что оно будет использовать Закон о ложных претензиях, основной гражданский инструмент правительства США для возмещения ложных претензий на федеральные средства и имущество, для подачи исков против подрядчиков и субподрядчиков правительства США, которые не соответствуют требованиям кибербезопасности конкретного контракта или гранта. Министерство юстиции США («Министерство юстиции») определенно не блефовало. За последние несколько месяцев Министерство юстиции объявило об урегулировании двух дел в соответствии с Законом о ложных претензиях, связанных с недостатками или искажениями в кибербезопасности, и ожидается, что их станет больше.

Таким образом, теперь крайне важно, чтобы компании, выполняющие государственные контракты и субподряды США, заранее оценивали свое соответствие федеральным требованиям кибербезопасности.

Инициатива Министерства юстиции по борьбе с кибермошенничеством

В октябре 2021 года заместитель генерального прокурора Лиза О. Монако объявила о запуске Министерством юстиции «Инициативы по борьбе с гражданским кибермошенничеством», в рамках которой, по ее словам, будут привлечены к ответственности физические или юридические лица, которые подвергают риску информацию или системы США, сознательно предоставляя несовершенные продукты кибербезопасности. или услуги, сознательно искажающие их методы или протоколы кибербезопасности или сознательно нарушающие обязательства по отслеживанию и сообщению об инцидентах и нарушениях кибербезопасности. Инициатива по борьбе с гражданским кибермошенничеством будет использовать Закон о ложных претензиях («FCA») для возбуждения дел, связанных с кибербезопасностью, против государственных подрядчиков, субподрядчиков и получателей грантов.

Закон о ложных претензиях

FCA является основным гражданским инструментом федерального правительства США для борьбы с мошенничеством против правительства.

Он возлагает ответственность на лиц и компании (как правило, федеральных подрядчиков и субподрядчиков), которые мошенническим путем получают платежи от федерального правительства США или уклоняются от них. В настоящее время правительство США вернуло более 70 миллиардов долларов США в соответствии с FCA.

Правоприменительная деятельность

За последние несколько месяцев Министерство юстиции объявило об урегулировании двух дел FCA, связанных с недостатками кибербезопасности со стороны государственных подрядчиков.

8 марта 2022 г. в первом разрешении Министерства юстиции по делу FCA, касающемуся кибербезопасности, с момента запуска Инициативы по борьбе с гражданским кибермошенничеством, Министерство юстиции объявило, что Comprehensive Health Services LLC («CHS») согласилась выплатить почти 1 миллион долларов США. для устранения утверждений о том, что он нарушил FCA, ложно заявив Государственному департаменту США («Штат») и ВВС США («ВВС США»), что он выполнил требования контракта, касающиеся предоставления медицинских услуг в штате и ВВС США. объектов в Ираке и Афганистане. Среди нарушений CHS, поставщик глобальных медицинских услуг, который заключил контракт на оказание медицинских вспомогательных услуг в учреждениях, подал претензии к штату в отношении стоимости защищенной системы электронных медицинских карт (EMR) для хранения всех медицинских карт пациентов., включая конфиденциальную идентифицирующую информацию американских военнослужащих, дипломатов, официальных лиц и подрядчиков, работающих и получающих медицинскую помощь. Однако CHS не сообщила государству о непоследовательном использовании защищенной системы EMR в течение семилетнего периода.

Затем, 8 июля 2022 года, Министерство юстиции объявило, что Aerojet Rocketdyne Inc. («Aerojet») согласилась выплатить 9 миллионов долларов США для устранения обвинений в том, что она нарушила FCA, предоставив ложную информацию о соблюдении ею требований кибербезопасности в некоторых контрактах с федеральным правительством, требующих, чтобы оборонные подрядчики защищать несекретную контролируемую техническую информацию. Было установлено, что компания Aerojet, которая поставляет двигательные и силовые установки для ракет-носителей, ракет, спутников и других космических аппаратов Министерству обороны США, Национальному управлению по аэронавтике и исследованию космического пространства («НАСА») и другим федеральным агентствам, побудила правительство заключать контракты, зная, что это не соответствует Положению об оборонных федеральных закупках 48 CFR § 252.204-7012 (DFARS) и Постановление о федеральных закупках НАСА 48 CFR § 1852.204-76 (NASA FARS), оба из которых были предварительными условиями договора. Например, один внешний аудит установил, что Aerojet соблюдает только 5 из 59 необходимых мер контроля в соответствии с DFARS, другой выявил недостатки с высоким риском, а третий смог проникнуть в сеть Aerojet в течение нескольких часов.

Дополнительные соображения

Эти случаи подчеркивают повышенный риск FCA, который соблюдение требований кибербезопасности представляет для государственных подрядчиков и субподрядчиков США.

Важно отметить, что ответственность должна возлагаться не на правительство, понесшее известную потерю данных, а скорее на то, выполняет ли соответствующий подрядчик или субподрядчик полный набор своих договорных обязательств перед правительством, включая существенные требования кибербезопасности.

Необдуманное предоставление ложных сведений о соблюдении договорных обязательств или преднамеренное согласие на включение определенных требований в контракт, но затем невыполнение этого требования влечет за собой ответственность в соответствии с FCA.

В дополнение к разрешению Соединенным Штатам самостоятельно преследовать виновных в мошенничестве, FCA позволяет частным лицам или «связям» (по сути, осведомителям), которым известно о прошлых или настоящих мошенничествах, совершенных против федерального правительства, подавать иски от имени правительства (так называемые иски «qui tam») в обмен на возможность участвовать в последующих финансовых расчетах. На самом деле, многие расследования и судебные иски Департамента юстиции по борьбе с мошенничеством являются следствием таких бессистемных действий.

Соответственно, подрядчики и субподрядчики должны обращаться к консультанту, чтобы понять свои обязательства в области кибербезопасности по существующим и будущим контрактам и субконтрактам с правительством США, обучать сотрудников, внедрять средства контроля информационной безопасности, такие как ограничения доступа и сети, разрабатывать планы реагирования на инциденты и стратегии выкупа, а также внедрять внутренние сообщения о нарушениях». ***(Karen Harbaugh, Richard Gibbon. Cybersecurity Compliance on U.S. Government Contracts and Subcontracts // Squire Patton Boggs (https://www.anticorruptionblog.com/cybersecurity/cybersecurity-compliance-on-u-s-government-contracts-and-subcontracts/#page=1). 19.09.2022).***

***

«Сотрудники малых и средних канадских организаций получили оценку «С» за свои знания в области кибербезопасности и информированность.

Рейтинг исходит от Страхового бюро Канады, которое после опроса 1525 работников компаний с менее чем 500 сотрудниками пришло к выводу, что фирмы медленно адаптируются ко все более частым и изощренным кибератакам.

Среди того, что бюро назвало «поразительными» выводами:

только треть респондентов (34%) заявили, что их компания проводит обязательное обучение по вопросам кибербезопасности;

только половина респондентов заявила, что их организация внедрила многофакторную аутентификацию;

только четверть респондентов (24%) заявили, что их работодатели проводят симуляции фишинговых электронных писем, чтобы повысить бдительность в киберпространстве.

Чуть менее трех четвертей респондентов (72%) заявили, что они сделали что-то, что могло позволить киберпреступнику получить доступ к компьютерным системам их компании. Например:

27% сказали, что используют один пароль для доступа к нескольким веб-сайтам, которые используют для работы;

23% используют общедоступный Wi-Fi, используя свой рабочий компьютер;

19% заявили, что загружают на свои рабочие устройства программное обеспечение/приложения, которые не были предоставлены их работодателем;

7% позволяют членам семьи или друзьям пользоваться своим рабочим компьютером; а также

5% сообщают свой рабочий логин или пароль по электронной почте или текстовым сообщениям.

Результаты опроса, получившие название Cyber Savvy Report Card, были опубликованы в преддверии октябрьского месяца осведомленности о кибербезопасности.

Чтобы повысить осведомленность, бюро запустило cybersavvycanada.ca, чтобы помочь владельцам малого бизнеса и их сотрудникам лучше понять угрозу кибератак и то, что они могут сделать, чтобы снизить свой риск.

«Каждый должен сыграть свою роль в снижении киберугроз на рабочем месте», — сказала Селесте Пауэр, исполнительный вице-президент страхового бюро по стратегическим инициативам и защите интересов. «Хотя киберстрахование является важным средством поддержки бизнеса в случае кибератаки, его следует рассматривать как один из компонентов комплексной стратегии снижения киберрисков, направленной на снижение уязвимости организации перед онлайн-угрозами».

По словам бюро, сотрудники также могут недооценивать роль, которую они играют в киберзащите своей организации. В нем отмечается, что 30% респондентов заявили, что не верят, что киберпреступники станут преследовать их на работе, а 28% респондентов заявили, что их работодатель несет исключительную ответственность за защиту своего рабочего места от киберугроз.

Двадцать один процент респондентов считают, что большинство кибератак незначительны и их легко устранить. «Реальность такова, — говорится в пресс-релизе бюро, сопровождающем результаты, — что они могут иметь разрушительные финансовые последствия». Ссылаясь на последний годовой отчет IBM об утечке данных, бюро отмечает, что в 2021 году средняя общая стоимость утечки данных для канадских организаций оценивалась в 7,3 миллиона долларов.

Страховое бюро заинтересовано в кибербезопасности клиентов с киберстрахованием. Согласно глобальному опросу, опубликованному в прошлом месяце, в результате роста требований и выплат страховщики повышают премии, ограничивают покрытие и требуют от клиентов ужесточить свою киберзащиту». ***(Howard Solomon. Canadian SMBs, employees criticized for poor cybersecurity practices // ITWC (https://www.itworldcanada.com/article/canadian-smbs-employees-criticized-for-poor-cybersecurity-practices/504284). 22.09.2022).***

***

«Счетная палата правительства выявила серьезные недостатки в области кибербезопасности в агентстве, отвечающем за надзор за ядерными запасами США.

В расследовании, опубликованном в четверг, наблюдательный орган обнаружил, что Национальное управление по ядерной безопасности (NNSA) полностью внедрило только четыре из шести основных требований кибербезопасности в своей традиционной ИТ-среде, которая включает компьютерные системы, используемые для разработки оружия.

В частности, в ходе аудита GAO обнаружило, что как NNSA, так и его подрядчики не полностью внедрили стратегию непрерывного мониторинга, поскольку в их стратегических документах отсутствовали ключевые рекомендуемые элементы.

«Без таких элементов NNSA и его подрядчики не имеют полного понимания своего состояния кибербезопасности и ограничены в своих возможностях эффективно реагировать на возникающие киберугрозы», — говорится в отчете GAO.

В рамках ИТ-среды ядерного оружия NNSA, которая относится к ИТ в системах вооружения или в постоянном контакте с ними, наблюдательный орган обнаружил, что агентство не разработало стратегию управления киберрисками, которая, по его словам, «вероятно ограничивает осведомленность NNSA о таких угрозах и реакцию на них».»

Директива NNSA по кибербезопасности требует, чтобы подрядчики контролировали меры кибербезопасности своих субподрядчиков.

Однако трое из семи подрядчиков не поверили, что это является договорной ответственностью, когда их спросили в GAO.

«Эти пробелы в надзоре как на уровне подрядчика, так и на уровне NNSA оставляют NNSA мало уверенности в том, что конфиденциальная информация, хранящаяся у субподрядчиков, эффективно защищена», — добавил наблюдатель в отчете». ***(John Hewitt Jones. Watchdog report identifies cybersecurity failings at National Nuclear Security Administration // FedScoop (https://www.fedscoop.com/watchdog-report-identifies-cybersecurity-failings-at-national-nuclear-security-administration/). 23.09.2022).***

***

«…Национальный институт стандартов и технологий (NIST) признает информационную безопасность и кибербезопасность отдельными областями карьеры. Тем не менее, между ними, безусловно, есть совпадение. Ниже приведены ключевые определения и различия каждого из них.

Что такое информационная безопасность?

В какой-то степени почти каждый хочет, чтобы его личная информация была в безопасности, а это означает, что доступ к ней и ее использование могут получить только уполномоченные лица. Это цель информационной безопасности (infosec).

Согласно NIST, информационная безопасность включает в себя защиту информации и информационных систем от несанкционированного использования. Поле направлено на обеспечение доступности, целостности и конфиденциальности.

Один из способов понять информационную безопасность по сравнению с кибербезопасностью — рассматривать поле как общий термин, включающий все данные, а не только данные, хранящиеся в киберпространстве. Это демонстрирует, как кибербезопасность является типом информационной безопасности, но эти две области не идентичны.

Группы информационной безопасности создают и внедряют политики и системы для защиты информации. Для крупных организаций требуются строгие системы безопасности для защиты клиентов.

Что такое кибербезопасность?

Жизнь в 21 веке означает, что большая часть данных хранится в компьютерных системах и сетях. Это относится почти к каждой отрасли, и информация должна быть защищена в высокой степени. Специалисты по информационной безопасности, специализирующиеся на кибербезопасности, несут ответственность за защиту этих данных.

NIST определяет кибербезопасность как защиту, предотвращение повреждения и восстановление услуг и систем электронных коммуникаций. Сюда входит информация, хранящаяся в этих системах, над защитой которой работают специалисты по кибербезопасности.

Кибербезопасность охватывает все, что связано с электронными системами и коммуникациями. В области кибербезопасности есть подкатегории, которые влекут за собой дальнейшую специализацию. К ним относятся безопасность облака, сети и критической инфраструктуры.

Самые большие различия

Может возникнуть путаница между информационной безопасностью и кибербезопасностью, поскольку большая часть информации, которую мы хотим хранить, защищать и передавать, существует в киберпространстве. Хотя кибербезопасность является частью информационной безопасности, некоторые аспекты информационной безопасности не входят в сферу кибербезопасности.

Информационная безопасность — это общий термин для создания и обслуживания систем и политик для защиты любой информации — цифровой, физической или интеллектуальной, а не только данных в киберпространстве.

Эксперт по информационной безопасности может разработать средства доступа к данным уполномоченными лицами или установить меры безопасности для обеспечения безопасности информации. Кибербезопасность, с другой стороны, сосредоточена на защите информации от кибератак, таких как программы-вымогатели и программы-шпионы.

Информационная безопасность и кибербезопасность во многом пересекаются. В дополнение к схожим методам обеспечения безопасности эти области также требуют аналогичного образования и навыков.

Общие методы обеспечения безопасности

Наиболее существенное совпадение между информационной безопасностью и кибербезопасностью заключается в том, что они используют модель триады CIA (конфиденциальность, целостность и доступность информации) для разработки политик безопасности.

Первым из триады является конфиденциальность, гарантирующая, что информация доступна и может быть изменена только авторизованными пользователями. Например, с точки зрения потребителя мы ожидаем, что интернет-магазины будут хранить и защищать наши данные, такие как данные кредитной карты, домашние адреса и другую личную информацию.

Во-вторых, целостность информации гарантирует, что она не была подделана и полностью надежна. Продолжая пример с интернет-магазином, данные, передаваемые между продавцом и вашим банком, должны быть защищены. В противном случае может возникнуть несоответствие между фактической стоимостью вашего товара и оплаченной вами суммой.

Наконец, доступность информации означает, что данные доступны, когда они вам нужны. Например, если вам нужно знать, сколько денег у вас на банковском счету, вы должны иметь доступ к этой информации.

Сопутствующее образование и навыки

Как минимум, для многих профессий в области информационной безопасности и кибербезопасности требуется степень бакалавра в области кибербезопасности, компьютерных наук, информационных технологий или смежных областей. Эти степени подготовят вас к базовым знаниям и навыкам, которые помогут вам получить работу в качестве аналитика, инженера, специалиста или тестировщика.

Эти карьеры также требуют знакомства с такими технологиями, как пользовательский интерфейс базы данных и программное обеспечение для запросов, программное обеспечение для мониторинга сети, защита от вирусов и разработка веб-платформы.

Многие специалисты по информационной безопасности и кибербезопасности используют схожие или взаимозаменяемые формулировки в своих должностных инструкциях. Это связано с тем, что работодателям часто нужны специалисты по информационной безопасности с широким набором навыков в области безопасности, в том числе в области кибербезопасности.

Роли в области информационной безопасности

Аналитик информационной безопасности

Обзор карьеры: поскольку на компьютерах хранится так много ценной информации, аналитики информационной безопасности часто выполняют те же задачи, что и аналитики кибербезопасности. Эти специалисты отвечают за планирование, внедрение, обновление и мониторинг мер безопасности для защиты компьютерных сетей и информации. Они также могут создавать и публиковать отчеты о показателях безопасности и утечках данных.

Средняя годовая зарплата: более 74 000 долларов США, согласно Payscale.

Специалист по информационной безопасности

Обзор карьеры: Роль специалиста по информационной безопасности аналогична роли аналитика по информационной безопасности. Хотя повседневные обязанности могут варьироваться в зависимости от конкретной должности, эти специалисты являются частью групп, которые разрабатывают и внедряют системы, стандарты и политики управления информационными рисками. Они также участвуют в оценке рисков и помогают пользователям получить доступ к базам данных.

Средняя годовая зарплата: более 76 000 долларов США, согласно Payscale.

Консультант по ИТ-безопасности

Обзор карьеры: Как консультант по ИТ-безопасности, вы используете свой опыт в области информационной безопасности, чтобы оценивать и рекомендовать улучшения информационной безопасности организации. В ваши обязанности может входить поддержка, внедрение и отслеживание улучшений конфиденциальности данных, систем управления доступом к идентификационным данным, управления кибербезопасностью и операций.

Средняя годовая зарплата: более 82 000 долларов США, согласно Payscale.

Роли кибербезопасности

Аналитик по кибербезопасности

Обзор карьеры: Аналитики по кибербезопасности сосредоточены на защите данных от кибератак. Эти специалисты выполняют обнаружение угроз и инцидентов и реагируют на утечки данных. В зависимости от работодателя аналитики по кибербезопасности могут разработать обучение по вопросам кибербезопасности и криминалистический анализ информационных систем.

Средняя годовая зарплата: более 77 000 долларов США, согласно Payscale.

Инженер по кибербезопасности

Обзор карьеры: Роль инженера по кибербезопасности обширна: он контролирует разработку процедур и политик кибербезопасности. Эта работа включает в себя создание и обслуживание брандмауэров для обеспечения безопасной передачи информации, разработку мер безопасности для защиты цифровых файлов, а также мониторинг и реагирование на нарушения безопасности. Если вам интересно, как стать инженером по кибербезопасности, начните со степени бакалавра или курса обучения кибербезопасности.

Средняя годовая зарплата: более 98 000 долларов США, согласно Payscale.

Тестер проникновения

Краткий обзор карьеры: Специалисты по тестированию на проникновение фактически являются хакерами, но с благими намерениями: улучшить методы защиты информации. С помощью смоделированных внутренних и внешних кибератак эти специалисты взламывают и эксплуатируют системы и получают доступ к конфиденциальной информации для выявления уязвимостей. Затем они разрабатывают и предлагают решения безопасности для устранения указанных уязвимостей. Они также обнаруживают слабые места в системе и предлагают улучшения для усиления защиты от вредоносных атак.

Средняя годовая зарплата: более 88 000 долларов США, согласно Payscale». ***(Brandon Galarita, Brenna Swanston. Information Security vs. Cybersecurity: What's The Difference? // Forbes Media LLC. (https://www.forbes.com/advisor/education/information-security-vs-cyber-security/). 23.09.2022).***

***

«Федеральное страховое управление Министерства финансов хочет знать, должна ли национальная программа страхования от киберугроз требовать от держателей полисов выполнения основных мер кибербезопасности, чтобы избежать морального риска.

«Должны ли меры кибербезопасности и / или кибергигиены требоваться от держателей полисов в соответствии со структурой?» Стивен Зейтц, директор Федерального страхового управления Министерства финансов, спросил в запросе на комментарий, который должен быть опубликован в Федеральном реестре в четверг. «Если да, то какие меры следует предпринять?»

Комментарии должны быть представлены в течение 45 дней после публикации уведомления. Те, кто заинтересован в обсуждении этого вопроса, также могут

принять участие в заседании Федерального консультативного комитета Министерства финансов США по страхованию в четверг днем.

Вопрос об эффективных мерах кибербезопасности является одним из нескольких, которые FIO и Агентство по кибербезопасности и безопасности инфраструктуры просят помочь подготовить отчет Конгрессу о достоинствах создания федеральной программы киберстрахования. Их усилия проистекают из рекомендации Счетной палаты правительства, которой Конгресс поручил изучить роль федерального правительства в киберстраховании в соответствии с Законом о государственной обороне от 2021 года.

GAO подчеркнуло возможность того, что федеральная программа страхования может создать искаженные стимулы в отрасли, особенно после атак программ-вымогателей по всей стране, но агентство передало эстафету FIO и CISA, чтобы дать окончательные рекомендации Конгрессу по этому вопросу.

В уведомлении Министерства финансов и CISA моральный риск описывается как «возможность того, что страховщики или держатели полисов могут пойти на неоправданный риск, полагаясь на ответ федерального страхования, или не внедрить средства контроля кибербезопасности».

Страхование обычно регулируется на уровне штата, но есть несколько примеров федеральных программ, в том числе Программа страхования от террористических рисков, за которой наблюдает Казначейство, и Национальная программа страхования от наводнений, которой управляет Федеральное агентство по чрезвычайным ситуациям.

NFIP требует страхового покрытия для определенных объектов недвижимости и финансируется за счет премий, но программа постоянно находится в долгах из-за огромных сумм, выплачиваемых после катастрофических ураганов. Поскольку эксперты предупреждают об урагане исторических масштабов, обрушившемся на штат Флорида, срок действия NFIP истекает, если Конгресс не утвердит его повторно к концу недели.

Модель TRIP, созданная после террористических атак 11 сентября, по существу обеспечивает страхование страховщиков, помогая им страховать держателей полисов в случае квалификационных инцидентов. Но существует ограничение в 100 миллиардов долларов на сумму, которую может выплатить правительство, и в уведомлении цитируется исследование CISA, опубликованное в 2020 году, в котором потенциальные убытки от одного кибер-инцидента оцениваются в диапазоне от 2,8 миллиардов до 1 триллиона долларов.

«Должна ли существующая федеральная программа страхования (например, NFIP или TRIP) или другие американские или международные механизмы государственно-частного страхования служить моделью или быть изменена для решения катастрофических киберинцидентов?» — спрашивает уведомление.

Согласно уведомлению, «FIO намеревается оценить потенциальные ответы федерального страхования, которые не входят в TRIP, но также рассмотрит, как потенциальные ответы могут взаимодействовать с TRIP или быть его частью». Это вызвало бы вопросы о том, следует ли считать определенные киберинциденты террористическими атаками.

Агентства также хотят получить ответы на множество других вопросов, например, будут ли страховщики с меньшей вероятностью покрывать события, которые привели к физическим последствиям, и какую сумму финансовых потерь следует считать «катастрофическими».

«Какие меры кибербезопасности наиболее эффективно уменьшат вероятность или масштабы катастрофических киберинцидентов?» уведомление также спрашивает. «Какие шаги может предпринять федеральное правительство, чтобы потенциально стимулировать или потребовать от держателей полисов принятия этих мер?» ***(Mariam Baksh. The Department's Federal Insurance Office—together with the Cybersecurity and Infrastructure Security Agency—is soliciting feedback in preparation for a report to Congress // Nextgov (https://www.nextgov.com/cybersecurity/2022/09/treasury-seeks-comment-how-structure-cyber-insurance-program/377793/). 29.09.2022).***

***

«Согласно новому исследованию Счетной палаты правительства, новая волна серьезных проблем национальной безопасности связана с цифровой информационной средой и продолжающимся распространением дезинформации и киберугроз в виртуальных сетях.

Отметив, что боевые действия и разведывательные операции Министерства обороны США в значительной степени основаны на сборе данных и взаимосвязанной информационной среде, официальные лица GAO выделили шесть областей, которые могли бы выиграть от усиления контроля и защиты данных.

Конкретные шесть областей цифровой среды Министерства обороны США, опрошенных исследователями GAO, включают: дезинформацию и дезинформацию; влияние на миссии и функции Министерства обороны США; субъекты угроз; действия угрозы; институциональные проблемы; и новые технологии.

Джозеф Киршбаум, директор по оборонным возможностям и управлению в GAO, сказал, что слияние этих шести факторов с годами усиливается и может усугубить действия по угрозам Министерству обороны.

«Слияние и взаимодействие киберпространства, информации, электромагнитного спектра и подобных тем играет центральную роль в оценке информационной среды в целом», — сказал он Nextgov.

Эти области угроз могут быть использованы для подрыва миссий и операций Министерства обороны США, в частности, посредством злонамеренной киберактивности против федеральных сетей, незаконного сбора данных и атак на электромагнитный спектр, на который полагаются многие военные бойцы Министерства обороны США.

Воздействие враждебных действий на информационную среду Министерства обороны варьируется от технологических последствий до негативного воздействия на персонал Министерства обороны.

Одной из актуальных тем, отмеченных в отчете, является воздействие на когнитивные основы людей, состоящие из убеждений, психического здоровья, эмоций и переживаний, и их ключевая роль в распространении вредоносной дезинформации, которая может подорвать национальную безопасность.

«Распространение вездесущей информации, дезинформации, дезинформации и недобросовестной информации побудило экспертов в области обороны начать изучение концепции когнитивной безопасности», — отмечается в отчете.

Хотя концепция когнитивной безопасности технически не нова, ее применению в отношении того, как военачальники — или кто угодно — — воспринимают информацию и последующее влияние на национальную безопасность, уделяется новое внимание. Киршбаум сказал, что влияние дезинформации играет «решающую» роль в когнитивной безопасности.

«Это предполагает более глубокое понимание того, как информация, поступающая из столь многих источников, может влиять на наши решения», — сказал он.

Кроме того, в отчете отмечается, что новые технологии, такие как искусственный интеллект, машинное обучение, квантовые вычисления и растущий Интернет вещей, могут как помогать, так и препятствовать операциям Министерства обороны как угрозы или возможности.

Киршбаум пояснил, что официальные лица Министерства обороны в первую очередь обеспокоены иностранными субъектами угроз из враждебных стран, таких как Россия и Китай. Однако он также отметил, что аналогичную тактику угроз используют экстремисты из числа бытовых воинствующих экстремистов.

«Министерство обороны должно продолжать искать способы защиты информации, систем и разума с помощью разрозненных областей безопасности, таких как информационная безопасность, безопасность операций, кибербезопасность, физическая безопасность и когнитивная безопасность», — говорится в отчете». ***(Alexandra Kelley. GAO identified six areas that require more oversight, as Defense warfighting operations and national security increasingly hinge on data security // Nextgov (https://www.nextgov.com/cybersecurity/2022/09/dods-digital-threats-are-increasingly-interconnecting-watchdog-warns/377530/). 22.09.2022).***

***

«Законодательство, направленное на повышение кибербезопасности с помощью программного обеспечения с открытым исходным кодом, вынесенное на голосование в комитете Сената по внутренней безопасности и делам правительства в среду, зависит от того, в какой степени федеральные агентства собирают спецификации программного обеспечения или SBOM от федеральных подрядчиков.

Закон о защите программного обеспечения с открытым исходным кодом от 2022 года предписывает директору Агентства кибербезопасности и безопасности инфраструктуры оценивать «компоненты программного обеспечения с открытым исходным кодом, прямо или косвенно используемые федеральными агентствами». Оценка должна быть «основана на легкодоступной и, насколько это практически возможно, машиночитаемой информации, такой как спецификации программного обеспечения, которые предоставляются Агентству или иным образом доступны через Интернет; реестры программного обеспечения, собранные в рамках программы непрерывной диагностики и смягчения последствий Агентства; и другую

общедоступную информацию о компонентах программного обеспечения с открытым исходным кодом», — говорится в тексте законопроекта.

SBOM обычно сравнивают со списком ингредиентов, которые потребители могут использовать при выборе продуктов питания. Сторонники говорят, что в зависимости от SBOM потребители программного обеспечения могут быть столь же рассудительными и избегать продуктов и услуг, использующих библиотеки кода — часто с открытым исходным кодом — которые могут быть связаны с огромным количеством известных уязвимостей или другими причинами для беспокойства. SBOM были объявлены важной функцией Исполнительного указа 14028, в котором предполагалось, что федеральные агентства вскоре могут потребовать от поставщиков критического программного обеспечения предоставлять SBOM в качестве условия для закупок.

Но в недавнем меморандуме Управления управления и бюджета, выпущенном для реализации ЕО, говорится, что агентства «могут» потребовать от SBOM действовать в качестве доказательства того, что поставщики следуют рекомендациям Национального института стандартов и технологий по безопасной разработке программного обеспечения. А торговые ассоциации индустрии программного обеспечения и основные поставщики информационных и коммуникационных технологий недавно выступили против усилий, которые могли бы направить агентства к требованию SBOM через Закон о разрешении на национальную оборону.

В опубликованном в четверг пресс-релизе председателя и высокопоставленного члена Комитета внутренней безопасности — авторов закона о безопасности с открытым исходным кодом, объявляющего об их законопроекте, SBOM вообще не упоминается.

В среду комитет также внесет пометку в S. 4828, Закон об управлении и повышении производительности Правительственного исполнительного совета. В соответствии с этим законом будет создан новый совет для упорядочения и устранения противоречий в деятельности правительственных исполнительных советов, в том числе состоящих, в частности, из финансовых директоров агентств, директоров по данным и директоров по информационным технологиям.

S. 4528, Закон об улучшении цифровой идентификации от 2022 г., который предоставит гранты для стимулирования государственных и местных органов власти к обеспечению цифровой совместимости учетных данных, таких как водительские права, также может выйти из комитета в среду». ***(Mariam Baksh. Success would depend to a significant degree on whether agencies require vendors of information and communications technology to provide a software bill of materials with their products and services // Nextgov (https://www.nextgov.com/cybersecurity/2022/09/senate-legislation-secure-open-source-software-relies-transparency-initiative/377722/). 27.09.2022).***

***

«Вопрос больше не в том, будет ли взломана ваша организация, а когда. Только в 2021 году 212,4 млн американских компаний пострадали от кибератак. Поскольку большинство сегодняшних наиболее разрушительных атак

происходят из-за скомпрометированных учетных данных, кибербезопасность стала серьезной проблемой для руководителей бизнеса.

Этот всплеск кибератак побудил провайдеров киберстрахования поднять свои взносы. И многие андеррайтеры ищут надежные средства управления привилегированным доступом (PAM), прежде чем оценивать свои политики, учитывая, что скомпрометированные учетные данные являются основной причиной атак. Хотя очевидно, что нет никакой замены надежной киберструктуре, страхование киберответственности часто служит последней линией защиты организации, когда все остальное терпит неудачу.

Что покрывает киберстрахование

Каждая компания сталкивается с кибер-рисками: чем крупнее организация, тем больше у нее уязвимостей. Кибер-риск проявляется в виде риска конфиденциальности, безопасности, операционного риска и риска обслуживания. Хорошей новостью является то, что эти виды рисков покрываются киберстрахованием.

Киберстрахование предназначено для защиты организации от основных рисков с помощью четырех страховых соглашений:

Ответственность за сетевую безопасность и конфиденциальность

Прерывание работы сети

Ответственность СМИ

Ошибка и упущения

Политики сетевой безопасности важны для большинства организаций, и покрытие часто включает затраты первой стороны и расходы, непосредственно понесенные в результате киберинцидента. Покрытие ответственности за конфиденциальность защищает организации от нарушений или нарушений, которые подвергают конфиденциальную информацию о клиентах и сотрудниках, а также организацию к ответственности. Перебои в работе сети, ответственность СМИ и освещение ошибок и упущений также следует учитывать в соответствии с потребностями бизнеса.

Надежный полис киберстрахования покрывает расходы первых лиц, расходы третьих лиц и расходы на киберпреступления.

Рост киберстрахования

Только в четвертом квартале 2021 года стоимость киберстрахования выросла на 130%, и ожидается, что эта цифра продолжит расти в течение следующих двух лет. Эти растущие страховые взносы заставляют многие организации сомневаться в необходимости и ценности киберстрахования. Согласно недавнему отчету о тенденциях рынка киберстрахования, к отраслям, предъявляющим наибольшее количество претензий по киберстрахованию, относятся производство, финансовые услуги и здравоохранение. Ни одна отрасль не застрахована от кибератак, и защита от кражи данных и киберпреступности в растущей цифровой экономике важна как никогда.

Это настолько важно, что Целевая группа по программам-вымогателям включила способы усиления киберстрахования в свой недавно выпущенный план защиты от программ-вымогателей: план действий по смягчению последствий программ-вымогателей, реагированию и восстановлению для малых и средних

предприятий. В плане рекомендуются специальные меры безопасности, которые в индустрии киберстрахования позволили снизить затраты на инциденты. В нем также признаются средства контроля, на которые страховщики активно обращают внимание в процессе андеррайтинга, включая:

Внедрение надежных резервных копий

Обучение по вопросам безопасности и реагированию на инциденты

Безопасность электронной почты развернута по всему предприятию

Расширенная защита конечных точек от вредоносных программ

Видимость и безопасность сети

Глядя на эти факторы, компании могут определить, подходит ли им полис киберстрахования. Но есть много факторов, которые по-прежнему влияют на рост премий: возрастающая изощренность субъектов киберугроз, увеличение стоимости атак программ-вымогателей и неспособность точно понять состояние безопасности клиента. Поскольку эти элементы настолько распространены, компаниям необходимо понимать весь объем того, что на самом деле охватывает их политика.

Что не покрывает киберстрахование

Киберстрахование обеспечивает финансовую защиту организаций в отношении их цифровых активов. Однако он не покрывает все возможные риски и затраты. Большинство политик исключают обновление систем после взлома, чтобы предотвратить будущие инциденты. Политики кибербезопасности также не покрывают потенциальную будущую прибыль, которая может быть потеряна, или потерю стоимости, вызванную кражей интеллектуальной собственности у компании. Из-за этих пробелов в политиках компаниям необходимо искать подходы к безопасности на основе идентификации, чтобы гарантировать, что они действительно безопасны и соответствуют их страховым требованиям.

PAM и MFA могут помочь удовлетворить требования киберстрахования

Повышение уровня кибербезопасности вашей организации начинается с защиты идентификационных данных. PAM — это механизм информационной безопасности, который защищает удостоверения с особым доступом или возможностями, выходящим за рамки обычных пользователей. По сути, инструменты PAM помогают гарантировать, что пользователи имеют доступ только к тем ресурсам, которые им необходимы для выполнения их работы — ни больше, ни меньше. Это позволяет организациям управлять правами доступа для лучшей видимости и контроля, а также проверять все, прежде чем предоставлять доступ к важным активам.

Это сводится к безопасности, эффективности ИТ-администрирования, соответствию требованиям и гибкости бизнеса — и PAM покрывает все это. Страховые агенты обращают внимание на элементы управления PAM при ценообразовании киберполисов. Они ищут способы, которыми организация обнаруживает привилегированные учетные данные и безопасно управляет ими, как они контролируют привилегированные учетные записи и средства, которые у них есть для изоляции и аудита привилегированных сеансов. PAM помогает организациям соблюдать GDPR, NIS, PCI DSS и другие нормативные акты, что, в свою очередь, помогает организациям соблюдать требования и предпосылки киберстрахования.

Многофакторная аутентификация (MFA) для привилегированных учетных записей важна для организаций любого размера, а также важна для соблюдения требований киберстрахования. Страховые компании хотят видеть MFA на месте, чтобы обеспечить безопасное подключение локально и в облаке. MFA — это важный метод управления доступом к важным приложениям и ресурсам.

Для защиты от программ-вымогателей и соблюдения базовых требований безопасности, используемых большинством киберстраховщиков, организациям необходимо применять многофакторную аутентификацию для удостоверений. Фактически, страховщики могут отклонить организацию, которая не обеспечивает соблюдение MFA. Наличие MFA перед привилегированными учетными записями — это не только требование для киберстрахования, но и настоящая передовая практика.

Следующие шаги

Самое важное, что организации могут сделать в борьбе с кибератаками, — это обучить свой персонал. Убедитесь, что никто не нажимает на фишинговые электронные письма, и проводите периодические проверки фишинговых и целевых фишинговых писем. Большинство провайдеров киберстрахования хотят, чтобы организации проводили обучение по вопросам безопасности не менее четырех раз в год.

Премии по киберстрахованию стремительно растут в результате увеличения числа кибератак. Хотя не у каждой организации есть средства для прохождения пути киберстрахования, это вариант для многих организаций, которые хотят создать резервную копию своих планов и структур безопасности. Киберстрахование должно быть дополнением к надежной программе кибербезопасности, а не вместо нее. Ключ к надежной кибербезопасности и удовлетворению страховых требований начинается с наличия надежной стратегии PAM и внедрения MFA. Сочетая это с мощной программой обучения по вопросам безопасности, предприятия могут соответствовать требованиям киберстрахования, экономить деньги и снижать риски». ***(Larry Chinski. How PAM, MFA Helps Organizations Meet Cyber Insurance Requirements // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/how-pam-mfa-helps-organizations-meet-cyber-insurance-requirements/). 27.09.2022).***

***

Країни ЄС та Великобританія

«Департамент цифровых технологий, культуры, СМИ и спорта (DCMS) подтвердил 30 августа 2022 года, что он будет продвигать новые жесткие правила и свод правил для повышения безопасности и устойчивости сетей и услуг электронных коммуникаций Соединенного Королевства против текущих и будущих киберугроз.

Новые правила будут распространяться на провайдеров сетей и услуг электронных коммуникаций общего пользования (операторов связи). При разработке как правил, так и кодекса были проинформированы основные регулирующие органы Соединенного Королевства, работающие с промышленностью, и это объявление было сделано в конце периода консультаций

по правилам. Окончательные проекты правил и кодекса будут представлены на рассмотрение парламента в ближайшее время, а новые правила, как ожидается, вступят в силу 1 октября 2022 года.

DCMS выделил следующие ключевые области правил; операторы связи должны убедиться, что они могут:

- защитить данные, обрабатываемые их сетями и службами, и защитить критически важные функции, которые позволяют им работать и управлять ими, в том числе путем выявления и оценки рисков для любого «пограничного» оборудования, которое напрямую подвергается воздействию потенциальных злоумышленников, например, радиомачты, Wi-Fi -маршрутизаторы и модемы, которые действуют как точки входа в сеть;
- защищать программное обеспечение и оборудование, которые отслеживают и анализируют их сети и службы, в том числе от вредоносных сигналов, поступающих в сеть, которые могут вызвать перебои в работе;
- иметь глубокое понимание своих рисков безопасности и способность определять, когда происходит аномальная деятельность, с регулярными отчетами для внутренних советов, чтобы гарантировать, что бизнес-процессы поддерживают безопасность; а также
- учитывать риски цепочки поставок, а также понимать и контролировать, кто имеет возможность доступа и внесения изменений в работу своих сетей и услуг для повышения безопасности.

В правилах устанавливаются контрольные точки и сроки, в течение которых операторы связи должны внедрять меры безопасности, которые будут периодически обновляться, чтобы не отставать от развивающихся киберугроз». ***(Mike Pierides, Michael R. Pfeuffer. UK Government to Introduce New Rules to Protect Telecoms Networks Against Cyberthreats // Morgan, Lewis & Bockius LLP. (https://www.morganlewis.com/blogs/sourcingatmorganlewis/2022/09/uk-government-to-introduce-new-rules-to-protect-telecoms-networks-against-cyberthreats). 01.09.2022).***

***

«Европейская комиссия хочет, чтобы повседневные подключенные устройства были менее уязвимы для кибератак, обязывая производителей усиливать безопасность на протяжении всего их жизненного цикла.

Закон о киберустойчивости, представленный в четверг в Брюсселе, направлен на то, чтобы стать мировым стандартом путем введения обязательных требований кибербезопасности для каждого продукта с цифровыми элементами, также известного как Интернет вещей, и сделать потребителей более информированными об аспекте кибербезопасности того, чем они занимаются. покупка.

«Когда дело доходит до кибербезопасности, Европа настолько сильна, насколько сильна ее самое слабое звено: будь то уязвимое государство-член или небезопасный продукт в цепочке поставок», — заявил в своем заявлении комиссар по внутреннему рынку Тьерри Бретон.

«Компьютеры, телефоны, бытовая техника, устройства виртуальной помощи, автомобили, игрушки… каждый из этих сотен миллионов подключенных продуктов

является потенциальной точкой входа для кибератаки. И все же сегодня большинство аппаратных и программных продуктов не при условии соблюдения любых обязательств в области кибербезопасности. Внедряя кибербезопасность по замыслу, Закон о киберустойчивости поможет защитить экономику Европы и нашу коллективную безопасность», — добавил он.

По данным Комиссии, атаки программ-вымогателей происходят каждые 11 секунд. Финансовые последствия атак программ-вымогателей оцениваются примерно в 20 миллиардов евро во всем мире в прошлом году, а глобальные ежегодные расходы на киберпреступления оцениваются в 5,5 триллионов евро.

Предложения Комиссии обяжут производителей учитывать кибербезопасность при проектировании и разработке своих продуктов и обеспечивать эффективное устранение любых уязвимостей в течение ожидаемого срока службы продукта или в течение пяти лет, в зависимости от того, что короче.

Они также должны будут активно сообщать об используемых уязвимостях и инцидентах, предоставлять обновления безопасности в течение как минимум пяти лет и предоставлять потребителям «четкие и понятные инструкции» по использованию продуктов с цифровыми элементами.

Производители, которые не соблюдают законодательство, будут либо временно, либо навсегда удалены с Единого рынка и/или будут оштрафованы на сумму от 2% до 5% от мирового оборота.

Предлагаемый закон должен быть одобрен парламентом и советом и вступить в силу через два года после окончательного одобрения». ***(Brussels plans to introduce cybersecurity requirements for connected devices // euronews (https://www.euronews.com/my-europe/2022/09/15/brussels-plans-to-introduce-cybersecurity-requirements-for-connected-devices). 15.09.2022).***

***

«Цифровые технологии все больше усложняют и трансформируют современные конфликты. Нынешняя война между Россией и Украиной, например, также разыгрывается в киберпространстве с участием множества государственных и частных субъектов. Это варьируется от формирования ИТ-армии украинских добровольцев до интенсификации поддерживаемых Кремлем злонамеренных кибероперацій и до предложения западными союзниками Украине помощи «по всему спектру; наступательные, оборонительные и [и] информационные операции».

Такие события имеют значение, поскольку они согласуются с более длительной историей киберконфликтов, протекающих параллельно и подпитывающих кинетические операции. Даже если киберизмерение конфликта, как отмечают эксперты, в настоящее время ограничено, существуют серьезные опасения по поводу дестабилизации международной обстановки безопасности, включая высокие риски эскалации. Эти риски также усугубляются потенциальным распространением кибератак, направленных против Украины, на другие страны, что может вызвать системные колебания в киберпространстве и за его пределами. Именно такие трансграничные последствия заставили Европейский Союз (ЕС) издать декларацию10 мая, решительно осудив злонамеренную киберактивность

Российской Федерации, нацеленную на спутниковую сеть KA-SAT, принадлежащую VIASAT, и способствовавшую военному вторжению в Украину.

Среди участников, усиливающих кибераспект конфликта, есть технологические компании, которые поддержали усилия Украины, развернув самые современные кибервозможности. К ним относится использование новых прорывных технологий (EDT) и, в частности, искусственного интеллекта (ИИ) в кибероперациях. Например, стало известно, что Украина использует программное обеспечение для распознавания лиц Clearview AI для идентификации российских солдат и украинцев, погибших на поле боя. В ответ на расширяющийся украинско-российский конфликт Vectra AI, лидер в области обнаружения угроз с помощью ИИ и ответ для гибридных и многооблачных предприятий, предлагает набор бесплатных инструментов и услуг кибербезопасности для организаций, которые считают, что они могут стать мишенью в результате этого конфликта. Использование этих киберинструментов в контексте продолжающейся войны является как новинкой, так и дополнительной сложностью, поскольку они могут вмешиваться в динамику конфликта или потенциально генерировать новую динамику конфликта.

Действительно, в более широкой картине повседневной практики кибербезопасности уже многие сложные проблемы смягчаются с помощью инструментов искусственного интеллекта и интеллектуальных решений, поскольку новые передовые возможности развиваются быстрыми темпами. События привлекли внимание экспертов во всем мире, которые анализируют потенциальное влияние конвергенции ИИ и кибербезопасности на такие темы, как слежка, национальная безопасность и геополитическая конкуренция за технологическое развитие.

Однако меньше внимания уделялось пониманию того, как ЕС и его различные институты и агентства решают многие технические, операционные и политические вопросы, связанные с этой растущей связью между ИИ и кибербезопасностью. Учитывая отсутствие аналитического внимания, эта статья направлена на изучение подхода ЕС к потенциальным вызовам и возможностям, возникающим в этой области политики, и выдвижению соответствующих политических решений.

Например, как технология двойного назначения, определенная Европейской комиссией как «подрывная», ИИ начинает играть жизненно важную роль в цифровом преобразовании ЕС и планировании кибербезопасности как в гражданской, так и в военной областях. Уже в декабре 2020 года Агентство Европейского Союза по кибербезопасности (ENISA) предупредило в отчете о проблемах кибербезопасности искусственного интеллекта, что ИИ может предоставить как возможности, так и проблемы. Они варьируются от кибербезопасности для ИИ до ИИ для поддержки кибербезопасности и злонамеренного и враждебного использования ИИ. Последняя категория включает в себя сложные атаки, такие как вредоносное ПО на основе ИИ, распределенные атаки типа «отказ в обслуживании» (DDoS) с использованием ИИ и расширенные кампании по дезинформации с использованием ИИ.

Действительно, ЕС признает бесчисленное количество возможных способов использования EDT в киберпространстве, которые могут коренным образом повлиять на ландшафт угроз в Европе. Стратегия кибербезопасности ЕС на

цифровое десятилетие от декабря 2020 года уже определила ключевые технологии, такие как искусственный интеллект, шифрование, квантовые вычисления и сети будущего поколения, как необходимые для кибербезопасности. В стратегии отмечается, что соображения кибербезопасности должны быть интегрированы во все цифровые инвестиции, связанные с вышеуказанными технологическими областями и целостностью их цепочек поставок. Выводы совета о развитии кибер-позиции Европейского Союза с мая 2022 года также подчеркивают «важность интенсивного использования новых технологий, особенно квантовых вычислений, искусственного интеллекта и больших данных, для достижения сравнительных преимуществ, в том числе с точки зрения операций, реагирующих на киберугроз».

Чтобы изучить ряд соответствующих инициатив, в статье сначала будут выделены несколько областей возможного интереса и изучены последствия быстро развивающихся систем ИИ в отношении политики, связанной с кибербезопасностью. Во-вторых, статья продолжается прослеживанием политических инициатив ЕС в обеих областях, представляющих интерес (политика ЕС в области искусственного интеллекта и кибербезопасности), в попытке выявить возможные связи между двумя областями в существующем политическом планировании, а также выяснить, существуют ли взаимосвязи между двумя областями. фигура в политическом мышлении ЕС. Наконец, в статье подробно рассматривается ряд многообещающих инициатив, начиная от подходов к регулированию и заканчивая исследовательскими и инновационными проектами. Последний потенциально мог бы дополнительно синхронизировать две области для разработки инновационной политики и практики в рамках развивающейся связи ЕС с ИИ и киберполитикой.

ИИ И КИБЕРПРОСТРАНСТВО: МНОГОМЕРНЫЕ ОТНОШЕНИЯ

Быстрорастущая область ИИ считается одним из самых важных достижений так называемой четвертой промышленной революции. Как подчеркивает Европейская комиссия в своем Предложении о постановлении, устанавливающем согласованные правила в отношении искусственного интеллекта (Закон об ИИ) от 2021 года, «за счет улучшения прогнозирования, оптимизации операций и распределения ресурсов […] использование искусственного интеллекта может способствовать достижению социально и экологически полезных результатов». и предоставить ключевые конкурентные преимущества компаниям и европейской экономике».

Однако этот потенциал делает кибербезопасность необходимой предпосылкой для безопасного развертывания этих систем для всех других социальных и экономических целей. Действительно, ЕС не упускает возможности подчеркнуть, что «кибербезопасность является неотъемлемой частью безопасности европейцев. Будь то подключенные устройства, электрические сети или банки, самолеты, государственные учреждения или больницы, которые они используют или часто посещают, люди заслуживают того, чтобы делать это, будучи уверенными в том, что они будут защищены от киберугроз». И в то же время кибербезопасность сама по себе является областью, которая, возможно, может использовать возможности систем искусственного интеллекта.

Инновационные решения на основе ИИ, от новых методов и алгоритмов, помогающих ускорить рутинные, но трудоемкие задачи, до поддерживаемых ИИ кибервозможностей, имеющих потенциальное стратегическое значение, все развернутые в настоящее время приложения и приложения, находящиеся на более ранних стадиях разработки, обладают функциями, которые могут произвести революцию в возможностях и операциях кибербезопасности. Ожидается, что по сравнению с обычными методами кибербезопасности они будут работать в большем масштабе и с большей скоростью., быть более адаптируемым и незаметным. Таким образом, они могут помочь улучшить показатели безопасности и усилить защиту цифровых систем от растущего числа изощренных киберугроз. Например, Pillsbury — глобальная юридическая фирма, специализирующаяся на технологиях, — и The Economist Intelligence Unit отметили в отчете, что 49% мировых лидеров считают ИИ лучшим инструментом для противодействия кибератакам со стороны государства. Широко распространенные системы машинного обучения и искусственного интеллекта в сфере кибербезопасности варьируются от алгоритмов обнаружения аномалий для выявления вредоносного трафика или поведения пользователей в режиме реального времени до алгоритмов обнаружения вредоносного ПО и спама нулевого дня и систем искусственного интеллекта, определяющих приоритеты угроз и предпринимающих автоматические действия по исправлению. Глобальное внимание исследований сосредоточено на многообещающих системах, способных проводить сложные киберкампании с новыми характеристиками, начиная от вредоносных программ, «способных к тактической адаптации», и заканчивая «расчетами ценности по отношению к стратегическим целям».

Тем не менее, возникают также новые риски и опасения, связанные со сложностями взаимодействия ИИ и агентов-людей: потенциальные технические сбои все еще развивающихся и еще не зрелых систем, не говоря уже о проблемах прозрачности, связанных с пониманием так называемого «черного мира». ящик» поведения интеллектуальных систем. Это приводит к ряду важных соображений, касающихся безопасности систем ИИ, уже развернутых в ряде секторов, таких как промышленность, здравоохранение, финансы, правоохранительные органы и безопасность границ, а также оборона. Эти системы в равной степени нуждаются в защите от кибербезопасности и защите от потенциальных атак со стороны самого ИИ. Они должны быть защищены не только от обычных угроз, но и от новых атак с использованием ИИ. Например, отравление — тип атаки, при котором злоумышленники передают алгоритму измененные данные, чтобы изменить его поведение в соответствии со своими целями.

ENISA описывает эту динамику в своем недавнем отчете о проблемах кибербезопасности искусственного интеллекта, проводя различие между кибератаками, нацеленными на ИИ, и кибератаками, поддерживаемыми ИИ. Эта разнонаправленная связь между кибербезопасностью и системами искусственного интеллекта определяет все более актуальную политическую связь, которая должна вызывать серьезную озабоченность ЕС. Интересно, что в отчете рекомендуется, чтобы ЕС уделял больше внимания тому, как ИИ и кибернексус проявляют себя в контексте меняющегося ландшафта угроз, а также в случае возможностей и операций в области кибербезопасности и киберзащиты. ЭНИСАВ отчете также

освещаются усилия агентства по активному картированию экосистемы ИИ и соответствующих проблем кибербезопасности путем рассмотрения таких проблем на различных этапах жизненного цикла ИИ. В частности, в отчете подчеркивается необходимость уделять первоочередное внимание безопасности цепочек поставок, инновациям и наращиванию потенциала, когда речь идет обо всех элементах безопасной, надежной и надежной европейской экосистемы искусственного интеллекта.

Мы утверждаем, что эти ключевые аспекты потенциально должны быть дополнительно отражены в предстоящей Политике киберзащиты ЕС 2022 года, чтобы ЕС был лучше подготовлен к «защите, обнаружению, защите и сдерживанию кибератак», а также в новой Европейской политике 2022 года. Закон о киберустойчивости и работа Объединенного киберподразделения (JCU). Учитывая признание ЕС того, что ИИ может быть как другом, так и врагом кибербезопасности, в следующем разделе задается вопрос о стадии разработки различных инициатив и инструментов ЕС, а также о согласованности текущих усилий ЕС.

СВЯЗЬ AI-CYBER NEXUS: НОВЫЕ ВЫЗОВЫ УПРАВЛЕНИЯ

ЕС, похоже, признает необходимость изучения оперативного использования систем ИИ для поддержки более широких целей и интересов кибербезопасности. Например, в своей Стратегии кибербезопасности ЕС на 2020 год Европейская комиссия предлагает создать сеть операционных центров безопасности (SOC) для анализа угроз на основе ИИ в форме Киберщита ЕС. Связь ИИ и кибербезопасности в ЕС можно условно разделить на две функциональные, но взаимосвязанные области, представляющие операционный и нормативный интерес.

Как отмечалось выше, системы искусственного интеллекта все чаще внедряются в повседневную деятельность групп кибербезопасности в частном и государственном секторах, помогая защищать фирмы и организации. Поставщики утверждают, что системы на нынешнем уровне технологического развития способны выполнять такие задачи, как обнаружение вторжений и угроз, курирование разведывательных данных или обнаружение уязвимостей, обеспечивая беспрецедентный уровень эффективности использования времени и ресурсов. Похоже, что именно на эти типы функций субъекты ЕС обратили внимание при разработке планов для Европейского киберщита и SOC, упомянутых выше. Работа этих SOC «очень требовательна и динамична, поэтому ИИ и, в частности, методы машинного обучения могут оказать неоценимую поддержку практикам», когда речь идет о быстром обнаружении, анализе и реагировании на инциденты кибербезопасности. Цель SOC — «улучшить обнаружение инцидентов, анализ и скорость реагирования с помощью современных возможностей искусственного интеллекта и машинного обучения».

Системы искусственного интеллекта готовы поддерживать операции в киберпространстве, которые выходят за рамки чисто оборонительной деятельности. Использование — пусть даже частичное — возможностей ИИ в наступательных кибероперациях считается следующим уровнем развития области кибербезопасности-ИИ. После конкурса DARPA Cyber Grand Challenge 2016 года на создание автоматических защитных систем, способных самостоятельно устанавливать исправления, многие относительно амбициозные оценки

предполагают будущие системы, способные «динамически бороться с злоумышленниками». Не ожидается, что такие системы появятся в краткосрочной перспективе, поскольку текущие исследования больше сосредоточены на улучшении совместной работы человека и машины., как показано в недавних проектах DARPA. ЕС очень заинтересован в том, чтобы следить за развитием событий. Это особенно важно, поскольку Китай и Россия работают над созданием соответствующих возможностей, включая программное обеспечение, «способное вести свои кибернаступления более автономно».

Стоит отметить, что ИИ не всегда создается специально для киберзащиты или нападения. Скорее, ИИ — это «технология общего назначения», универсальная технология, которая со временем «находит широкое применение, находит множество применений и имеет множество побочных эффектов». Политики трудно предсказать такие побочные эффекты, не говоря уже о регулировании, и требуют адаптивных форм управления, способных учитывать расширенные и непредсказуемые варианты использования, а также значительную степень организационной адаптивности. С точки зрения безопасности это означает постоянное расширение и углубление поверхности уязвимостей, намного превосходящее то, что происходило с обычными процессами цифровизации предыдущих десятилетий.

Одним из таких примеров является открытие многих алгоритмов для публичного использования, часто в развлекательных или коммерческих целях. Социальные сети недавно были заполнены изображениями публичного использования DALL-E mini, причем модель была доступна для общественности для использования с забавными, а иногда и странными результатами. Несмотря на результаты публичных экспериментов, опасность популяризации существует, особенно потому, что коммерциализация происходит в среде, где дезинформация уже давно возведена в ранг общественной угрозы и даже угрозы демократическим системам. Кроме того, стоит задаться вопросом, какие последствия демократизация доступа и использования готовых систем ИИ может иметь для кибербезопасности и обороны, особенно с учетом расширения поверхности уязвимости, сопровождающего широкое развертывание ИИ в гражданских и военных целях, поскольку описано выше.

Готов ли ЕС реагировать и противодействовать текущим и будущим возможностям и угрозам, исходящим от связи ИИ и кибербезопасности? И какие действия следует предпринять в отношении безопасности и защиты продуктов, инвестиций, инноваций, геополитической конкуренции за развертывание систем и многого другого?

ОТВЕТЫ ЕС: СОЕДИНЯЯ ТОЧКИ?

ЕС предпринял регуляторные, политические и операционные инициативы, имеющие особое значение для взаимосвязи ИИ и кибербезопасности. Они являются частью недавних усилий по общей консолидации технологического лидерства и суверенитета ЕС в важнейших технологических областях, а также его экономической конкурентоспособности и стратегической автономии в области безопасности и обороны.

РЕГУЛЯТОРНЫЕ И ПОЛИТИЧЕСКИЕ ВМЕШАТЕЛЬСТВА

ЕС рассматривает кибербезопасность как предварительное условие и как средство для достижения целей устойчивости, технологической автономии и лидерства: в Стратегии кибербезопасности 2020 г. отмечается, что «предстоящее десятилетие — это возможность ЕС лидировать в разработке безопасных технологий по всему миру. цепь."

В стратегии также отмечается необходимость новых технологических инноваций и промышленной политики для достижения этих целей. Однако этот перспективный технологический и промышленный подход должен сопровождаться (гео) стратегическим мышлением и конкретными действиями. Более того, стратегия обещает интегрировать кибербезопасность в цифровые инвестиции и разработку «ключевых технологий, таких как искусственный интеллект (ИИ), шифрование и квантовые вычисления» с использованием стимулов, обязательств и ориентиров. Неудивительно, что Стратегический компас ЕС по безопасности и обороне на 2022 г. подкрепляет такие идеи, отмечая важность EDT в киберпространстве и для киберзащиты, отмечая разработку и «интенсивное» использование новых технологий, таких как ИИ, большие данные и квантовые вычисления, для «достижения сравнительных преимуществ с точки зрения операций, реагирующих на киберугрозы и информационное превосходство».

Эти устремления сопровождаются формирующейся нормативно-правовой архитектурой ЕС, в том числе предложенным Комиссией проектом Закона об искусственном интеллекте ; Закон о данных ; переход от Директивы о сетевой и информационной безопасности (NIS) к ее продолжению, предложение о Директиве NIS 2 (в настоящее время находится на стадии переговоров); недавно представленный пакет цифровых услуг, состоящий из Закона о цифровых услугах (DSA) и Закона о цифровых рынках (DMA); и предстоящий Закон о киберустойчивости (CRA). Они дополняются рядом оперативных элементов, ориентированных на создание и развертывание возможностей.

Тем не менее, вышеупомянутая регулирующая архитектура также характеризуется иногда конфликтующим разделением полномочий между субъектами ЕС, а именно Европейской комиссией, Европейскими службами внешних действий, государствами-членами и агентствами ЕС, которым поручено разрабатывать политику в конкретной области, в первую очередь ENISA. Показательным примером является политика безопасности и обороны ЕС. Согласно определению Договора о Европейском Союзе и Договора о функционировании Европейского Союза, ЕС не обладает компетенцией в области обороны, а соответствующие области безопасности являются исключительной компетенцией государств-членов ЕС. Это создает разногласия в общих регулятивных и политических результатах, которые часто окрашиваются различными причинами в подходе к гражданским вопросам, вопросам безопасности и обороны и особенно к военному использованию этих систем. Однако обнадеживает то, что попытки преодолеть разрозненное мышление и наполнить предполагаемые политические инициативы определенной степенью согласованности теперь пользуются решительной поддержкой.

В этом отношении несколько военно-гражданских проектов, ориентированных на ИИ, заслуживают дальнейшего изучения. Например, План

действий Комиссии по синергии между гражданской, оборонной и космической промышленностью определяет подрывные технологии, включая ИИ, как вызывающие сдвиг парадигмы как в гражданской, так и в военной сферах: «Термин «подрывная технология» относится к технологии, вызывающей подрыв или сдвиг парадигмы, то есть радикальное, а не постепенное изменение. Разработка такой технологии сопряжена с «высоким риском, высоким потенциальным воздействием», и эта концепция в равной степени применима к гражданскому, оборонному и космическому секторам».

В то же время, поскольку Еврокомиссия контролирует различные инструменты, в том числе инновационные фонды, такие как программы Horizon Europe и DigitalEurope, в этом довольно жестком разделении компетенций стали появляться разногласия, а усилия по координации и движению к большей согласованности продвигаются даже если поэтапно.

Например, институты ЕС, и особенно Европейская комиссия, предприняли важные шаги для повышения амбиций блока в отношении лидерства ИИ. Комиссия стала ключевой движущей силой и определяющей повестку дня для более последовательного подхода к промышленной и технологической политике в области ИИ. Его план, изложенный в Белой книге по ИИ выпущенный в феврале 2020 года, должен был стимулировать исследования и инновации ЕС, а также его технологические и промышленные возможности в этом ключевом стратегическом секторе. Хотя в Белой книге специально исключены вопросы безопасности и обороны, Белая книга указывает на цель ЕС по созданию прочной технологической и промышленной базы для исследований и разработок в области ИИ. В документе предполагается, что ЕС мог бы объединить свои «технологические и промышленные возможности с высококачественной цифровой инфраструктурой и нормативно-правовой базой», уделяя пристальное внимание фундаментальным ценностям. Основными строительными блоками, предложенными в официальном документе, являются «экосистема совершенства» и «экосистема доверия».

Для создания передовой экосистемы Европейская комиссия предлагает оптимизировать исследования, развивать сотрудничество между государствами-членами и увеличивать инвестиции в разработку и внедрение ИИ. Эти действия основаны на Скоординированном плане по искусственному интеллекту от декабря 2018 г. (обновленном в 2021 г.). Для создания экосистемы доверия Европейская комиссия предлагает варианты создания правовой базы, направленной на устранение рисков для основных прав и безопасности. Это следует за работой Группы экспертов высокого уровня по искусственному интеллекту, созданной в июне 2018 года, и Руководством группы по этике для надежного ИИ; Подход «надежного ИИ» теперь реализован в Законе об ИИ.

Важно отметить, что в официальном документе кибербезопасность упоминается только дважды в основной части текста и один раз очень кратко в сноске, касающейся потенциального злонамеренного использования. Связь ИИ и кибербезопасности в основном и кратко рассматривается в связи с вопросами, связанными с безопасностью и ответственностью за продукцию, а также «проблемами, связанными с применением ИИ в критически важных инфраструктурах или злонамеренным использованием ИИ». Что касается концепции

безопасности, в официальном документе подчеркивается тот факт, что использование ИИ в продуктах и услугах может порождать риски, которые в настоящее время не учитываются в законодательстве ЕС, в том числе риски, подобные киберугрозам. Опыт ENISA по оценке ландшафта угроз ИИ также сводится к одному короткому предложению.

Следовательно, разные приоритеты и атрибуты, связанные с отдельными технологическими и цифровыми областями — в данном случае кибербезопасностью и новыми технологиями — отражаются в соответствующей фрагментации среди предлагаемых политических решений. По этой причине зачастую различные политические инициативы насыщены различной логикой, а взаимозависимость между секторами игнорируется. Одним из таких примеров является взаимозависимость между безопасностью, в частности кибербезопасностью, и безопасностью систем. И все же такие точки функциональной взаимозависимости между двумя сферами возникают все чаще, и вопрос для ЕС становится вопросом соединения точек.

Что касается кибербезопасности, нацеленной на ИИ, пример этой разницы между обоснованиями можно проиллюстрировать на примере изучения обсуждаемых в настоящее время нормативных предложений в области кибербезопасности и регулирования ИИ, а именно Директивы NIS 2 и Закона об ИИ. Первые пытаются прояснить условия кибербезопасности организаций, деятельность которых считается критически важной для бесперебойного функционирования политической и социально-экономической системы, путем введения обязательств по отчетности о происшествиях. Они охватывают широкий спектр областей, включая электричество, банковское дело, транспорт, цифровую инфраструктуру и государственное управление. Большинство секторов, входящих в сферу критической инфраструктуры, являются потенциальными целями для злонамеренной деятельности, исходящей из киберпространства, в силу их растущей зависимости от киберфизических систем для их дальнейшей работы. Такие промышленные системы управления, управляющие критически важными инфраструктурами, все чаще полагаются на автоматизацию для эффективной работы и, следовательно, становятся частью расширенной поверхности уязвимостей, связанных с ИИ. Тем не менее, в проекте предложения Европейской комиссии нет ссылок на системы с поддержкой ИИ или соответствующие положения.

В проекте Закона об искусственном интеллекте прямо упоминаются системы критической инфраструктуры, а также системы, задействованные в отправлении правосудия и в демократических процессах, включая выборы. В нем также неоднократно упоминается кибербезопасность продуктов, подверженных высокому риску злонамеренной деятельности, включая отравление данных или атаки злоумышленников, при этом ссылки обычно сгруппированы вместе с требованиями к точности и надежности. Закон возлагает ответственность за выполнение таких требований, от которых зависит безопасность развернутых продуктов, на производителей, а также на тех, кто размещает системы на рынке. Хотя в тексте отсутствуют явные ссылки на аспекты кибербезопасности при разработке, в нем уточняется, что продукты, соответствующие процессам кибербезопасности ЕС, как указано в Положение об ENISA и о сертификации кибербезопасности

информационно-коммуникационных технологий от 2019 года (Закон о кибербезопасности) может считаться отвечающим требованиям Закона об искусственном интеллекте.

В целом, NIS 2 не содержит положений о кибербезопасности систем ИИ, развернутых для функционирования критически важных инфраструктур, несмотря на то, что требования кибербезопасности этих систем отличаются от обычных операций кибербезопасности из-за различного характера угроз, с которыми сталкиваются указанные системы. Тем не менее, Закон об ИИ устанавливает некоторую связь между нарушениями безопасности и постоянной опасностью кибератак. Таким образом, исходя из предположения, мы можем предположить, что Закон об ИИ обеспечит определенную степень киберзащиты в случае кибератак на крупномасштабные системы, зависящие от ИИ. В этом смысле Закон об ИИ, похоже, делает еще один шаг в направлении киберзащиты систем ИИ. Ответственность за кибербезопасность действует в основном ex ante, хотя положения о послерыночном мониторинге и отчетности по «любое серьезное происшествие или неисправность» включены в предложение. Тем не менее, остается неясным, где ответственность за реагирование на такие потенциальные возможности и восстановление после них — особенно вызванных злонамеренной деятельностью — лежит между частными поставщиками и государственными органами на национальном уровне или уровне ЕС.

ОПЕРАЦИОННЫЕ ВОЗМОЖНОСТИ И СТРУКТУРЫ

ЕС также приступил к процессу формирования европейской экосистемы кибербезопасности, о чем свидетельствует недавнее распространение институциональных структур и процессов. Последние члены институциональной семьи ЕС в киберсфере — недавно созданный Европейский центр промышленной, технологической и исследовательской компетенции в области кибербезопасности и Сеть национальных координационных центров (или Центр компетенций и сеть), а также предложенный Комиссией JCU — все включают в некоторой степени исследование или использование возможностей, поддерживаемых ИИ.

В положении о создании Центра компетенций признается, что «Союзу по-прежнему не хватает технологических и промышленных мощностей и возможностей, чтобы автономно обеспечить безопасность своей экономики и критически важных инфраструктур и стать мировым лидером в области кибербезопасности». Примечательно, что помимо подчеркивания необходимости дальнейшей стратегической автономии в областях, связанных с кибербезопасностью, центр выявил недостаточный уровень стратегической и устойчивой координации и сотрудничества между различными заинтересованными сторонами, включая отрасли, исследовательские сообщества в области кибербезопасности и правительства. По этой причине центр призван стать «основным инструментом ЕС для объединения инвестиций в исследования в области кибербезопасности, технологий и промышленного развития, а также для реализации соответствующих проектов и инициатив».

Среди других координационных задач центр будет принимать стратегические инвестиционные решения и объединять ресурсы ЕС, его государств-членов и, косвенно, промышленности для улучшения и укрепления потенциала технологий и

промышленной кибербезопасности, укрепляя открытую стратегическую автономию ЕС. Это включает в себя поддержку проектов путем реализации частей кибербезопасности Horizon Europe, программы DigitalEurope и других фондов ЕС, а также разработку стратегических рекомендаций для исследований, инноваций и развертывания в области кибербезопасности.

Центр сопровождается сетью национальных координационных центров, которым поручено поддерживать сообщество кибербезопасности на национальном уровне и управлять частями доступного финансирования при определенных условиях. Интересно, что создание Центра компетенций и Сети следует за развитием четырех инновационных пилотных проектов, финансируемых ЕС, направленных на решение различных аспектов проблем координации между сообществами кибербезопасности, такими как частный сектор, малые и средние предприятия, исследования, и академические круги.

Например, в то время как CyberSec4Europe экспериментирует с новыми структурами управления, его коллега по проекту SPARTA работает над развитием возможностей в рамках связи AI-кибербезопасности, в частности таких возможностей, как автономные самозащищающиеся системы. Учитывая привилегированное положение соответствующих проектов в разработке и реализации Центра компетенций и Сети, можно было бы уделить больше внимания внедрению ИИ, а также других EDT в исследования и инновации в области кибербезопасности в ЕС.

Еще одна возможность, о которой стоит упомянуть, содержится в Рекомендации Комиссии от 2021 года, за которой последовало молчаливое одобрение Совета, по созданию JCU для координации всех существующих агентств кибербезопасности ЕС и возможностей на уровне ЕС, чтобы поддерживать потенциальные меры реагирования на киберинциденты. Действительно, следующий список организаций, которые рекомендованная структура стремится координировать, впечатляет, еще раз демонстрируя сильно фрагментированную экосистему ИИ-кибербезопасности в ЕС и настоятельную необходимость соединить точки:

С оперативной точки зрения эта существующая архитектура включает План скоординированного реагирования на крупномасштабные инциденты и кризисы в области кибербезопасности («План»), сеть CSIRT и сеть Европейской организации по связи с киберкризисами (EU CyCLONe), а также Европейскую сеть по борьбе с киберпреступностью. Центр (EC3) и Объединенная рабочая группа по киберпреступности (J-CAT) при Агентстве Европейского Союза по сотрудничеству правоохранительных органов (Европол), а также Протокол реагирования на чрезвычайные ситуации правоохранительных органов ЕС (EU LE ERP). Группа сотрудничества ННГ, Центр разведки и ситуации ЕС (EU INTCEN), набор инструментов кибердипломатии и проекты, связанные с киберзащитой, запущенные в рамках Постоянного структурированного сотрудничества (PESCO), также вносят свой вклад в политику и оперативное сотрудничество в различных сообществах кибербезопасности. Европейское агентство кибербезопасности (ENISA),

Соответственно, объем информации и разведывательных данных, накопленных, но неэффективно переданных между субъектами, в течение

длительного времени беспокоил организации и должностных лиц ЕС, и именно этот пробел в обмене информацией внутри ЕС поможет смягчить JCU. Среди прочего, рекомендация направлена на создание ранее упомянутой сети SOC, чтобы облегчить обмен информацией в этой обширной экосистеме заинтересованных сторон: «вклад в Объединенное киберподразделение должен позволить участникам укрепить существующие сети, такие как сеть CSIRT и ЕС. CyCLOne, предоставляющий им безопасные инструменты обмена информацией и улучшенные возможности обнаружения (например, центры обеспечения безопасности, «SOC») и позволяющий им использовать доступные операционные возможности ЕС».

В тексте также описывается создание «виртуальной платформы, состоящей из инструментов для совместной работы и безопасного обмена информацией». Эти инструменты будут использовать огромное количество информации, собранной через European Cyber Shield, включая SOC и центры обмена и анализа информации (ISAC). Именно через эту предполагаемую сеть SOC и ISAC ЕС стремится задействовать последние достижения в области использования ИИ для обнаружения аномалий и угроз и внедрить эти инструменты в возможности на уровне ЕС, разработанные в будущем.

ВЫВОД

ЕС преследует две цели: создать надежную архитектуру кибербезопасности в рамках всего блока и использовать преимущества ИИ для более широкой социальной и экономической (кибер) безопасности и обороны. Тем не менее, если цель состоит в том, чтобы обеспечить кибербезопасное развертывание систем и услуг ИИ, и чтобы оба аспекта ИИ для кибербезопасности и кибербезопасный ИИ занимали видное место в политике и операционных повестках дня ЕС, соединяя точки между различными инициативами, процессами и заинтересованными сторонами. имеет первостепенное значение. Требуется целостный взгляд на взаимосвязь ИИ и кибербезопасности.

Этого можно достичь с помощью нового межведомственного и стратегического мышления, чтобы проложить путь к конкретным действиям в связке ИИ и кибербезопасности, особенно с точки зрения лучшего понимания и снижения рисков постепенного использования систем и услуг ИИ в ключевых областях, таких как здравоохранение, транспорт, критическая инфраструктура, безопасность и оборона. Крайне важно усилить кибербезопасность ИИ и сохранить подотчетность в интеллектуальных системах. Кроме того, поскольку количество кибератак с использованием ИИ растет, ЕС и его государства-члены в партнерстве с частным сектором должны быть готовы реагировать на растущий спектр рисков и угроз кибербезопасности, связанных с ИИ, а также обладать возможности и опыт, необходимые для смягчения таких проблем». ***(Raluca Csernatoni, Katerina Mavrona. The Artificial Intelligence and Cybersecurity Nexus: Taking Stock of the European Union's Approach // Carnegie Europe (https://carnegieeurope.eu/2022/09/15/artificial-intelligence-and-cybersecurity-nexus-taking-stock-of-european-union-s-approach-pub-87886). 15.09.2022).***

***

«…в отчете, опубликованном в прошлом месяце Департаментом цифровых технологий, культуры, СМИ и спорта (DCMS), содержатся некоторые тревожные указания относительно потенциальной ответственности британских предприятий в результате кибератаки. В отчете обобщается опыт ряда предприятий, недавно подвергшихся серьезной кибератаке, и он был заказан DCMS в рамках продолжающегося исследования, направленного на то, чтобы помочь предприятиям понять угрозы кибербезопасности, с которыми они сталкиваются. Хотя некоторые из ключевых выводов отчета, возможно, не являются самыми информативными (например, консенсус в отношении того, что киберпреступность представляет собой значительный и растущий риск для бизнеса), более пристальный взгляд на отдельные тематические исследования дает некоторые поучительные и предостерегающие практические выводы.

Человеческий риск

Самое поразительное, что 70% предприятий сообщили либо о неадекватном обучении персонала в отношении киберрисков, либо о проведении более тщательного обучения после взлома. Учитывая, что подавляющее большинство кибератак для успеха по-прежнему полагаются на человеческую ошибку (например, сотрудник-получатель щелкает вредоносную ссылку в электронном письме), надежная и тщательная программа обучения персонала является одним из самых основных и фундаментальных инструментов управления рисками. В отчете подчеркивается тот факт, что многие компании по-прежнему рассматривают кибербезопасность исключительно как ИТ-проблему, которой можно управлять с помощью защитного программного обеспечения. Это ошибочное мнение может подпитываться тем, что сообщения о кибератаках часто описываются как «изощренные». Скорее всего, это не так.

Взаимодействие с советом директоров

Не меньшее беспокойство вызывает тот факт, что половина предприятий в отчете указали на неудовлетворительное участие совета директоров / высшего руководства в отношении кибербезопасности. Отсутствие реальной ответственности совета директоров и надзора за управлением киберрисками компании не только подвергает компанию и самих директоров потенциальной ответственности за ущерб, понесенный в результате нарушения, но также является упущенной возможностью привить подлинную культуру кибербезопасности. осведомленность и снижение рисков в бизнесе. Еще в 2016 году, когда Управление Комиссара по информации наложило на TalkTalk рекордный на тот момент штраф в размере 400 000 фунтов стерлингов за недостатки в кибербезопасности, Комиссар по информации воспользовался этой громкой возможностью, чтобы подчеркнуть, что штраф должен действовать как «предупреждение другим о том, что кибербезопасность это не проблема ИТ, это проблема совета директоров».

Плохая доставка третьими лицами

Часто недооцениваемая область риска обнаруживается в том факте, что половина предприятий сообщили о сбоях в работе поставщиков ИТ-услуг, с которыми они работали. Эти сбои (некоторые из которых были причиной самого нарушения) включали неправильно настроенное программное обеспечение, задержки в уведомлении бизнеса о нарушении, неверную информацию о причине

нарушения, а также отсутствие реакции и поддержки в устранении нарушения. Это дает полезную иллюстрацию важности тщательной должной осмотрительности при назначении поставщиков услуг. Надежный процесс закупок, который проверяет качество и послужной список потенциальных поставщиков услуг, имеет решающее значение, равно как и постоянный мониторинг для обеспечения качества предоставления услуг и эффективной защиты. Безоговорочная зависимость от поставщика услуг.

Отсутствие базовой сертификации

Треть предприятий подтвердили, что на момент взлома у них не было какой-либо базовой сертификации кибербезопасности (например, предоставленной поддерживаемой правительством схемой Cyber Essentials, которая помогает предприятиям защищаться от наиболее распространенных кибератак). Получение такой аккредитации — один из самых простых и очевидных способов для компаний продемонстрировать, что они предприняли конкретные шаги, чтобы начать понимать свои киберриски и управлять ими.

Поведение после нарушения

Очень немногие организации, участвовавшие в исследовании, предприняли формальные «извлеченные уроки» после взлома. Мало того, что такие упражнения предоставляют прекрасную возможность для бизнеса значительно снизить свою подверженность риску в будущем, но маловероятно, что они спровоцируют гнев клиентов/рынка и осуждение регулирующих органов больше, чем неспособность извлечь уроки из прошлых нарушений и исправить их (и, действительно, от нарушений, от которых пострадали другие лица, в той мере, в какой они становятся достоянием общественности).

Другие важные моменты

Несмотря на вышеперечисленные проблемные области, тематические исследования также содержат некоторые примеры передовой практики. Например, совет одного респондента, пострадавшего от атаки программы-вымогателя, уже использовал политику, запрещающую никогда не платить требования о выкупе, а это означало, что жизненно важное время отклика не использовалось для принятия решения о том, платить ли выкуп. Решение о том, платить выкуп или нет, связано с рядом юридических и практических соображений, которые требуют времени для проработки и часто вызывают бурные дискуссии и разногласия за столом заседаний совета директоров. Поэтому гораздо предпочтительнее, чтобы такие обсуждения проводились в рамках планирования реагирования компании на нарушения, а не сразу после нарушения.

Следует отметить два важных ограничения ценности выводов, представленных в отчете. Во-первых, ни одно из взломов не касалось личных данных, поэтому никому из респондентов не пришлось заморачиваться с отчетностью перед регулирующими органами. Такая отчетность и часто сопровождающая ее огласка являются одними из самых сложных аспектов многих серьезных кибератак. Во-вторых, ни в одном из тематических исследований не участвовал внутренний злодей. Хотя такие внутренние нарушения менее распространены, чем внешние атаки, они неизменно создают дополнительные

сложности и потенциально более опасны, поскольку инсайдер знает, где находится наиболее ценная информация, и может не торопиться с доступом к ней.

В заключение, хотя в отчете и говорится о том, что многие организации по-прежнему не реализуют некоторые из самых элементарных мер по управлению киберрисками, несмотря на то, что кибератаки постоянно возглавляют списки ключевых бизнес-угроз на протяжении нескольких лет, он также дает некоторую уверенность. Ни одна из кибератак, рассмотренных в тематических исследованиях, не была особенно новой, и ни одна из вышеперечисленных проблем управления рисками не является новой или неожиданной. Таким образом, тщательное рассмотрение вышеуказанных основных вопросов поможет компаниям и их советам директоров обрести большую уверенность в том, что, когда придет время (а оно наступит рано или поздно), они смогут ответить «да» на важнейший вопрос, на который они обращают внимание. Столкнется». ***(Lawson Caisley. Cyber security breaches: how would you answer the crucial question? // White & Case LLP (https://www.whitecase.com/insight-alert/cyber-security-breaches-how-would-you-answer-crucial-question). 16.09.2022).***

***

«NIS2 (Сетевая и информационная безопасность 2) и DORA (Закон о цифровой операционной устойчивости) будут опубликованы в ближайшие месяцы. Директива NIS2 и регламент DORA — это две крупные и важные европейские меры кибербезопасности. Директива NIS2 означает расширение количества секторов, которые должны соблюдать обязательства по кибербезопасности. Меры правоприменения расширяются, как и обязательства по отчетности.

Кроме того, появятся «обязательства руководства». Управление в рамках NIS2 будет означать, что политика кибербезопасности явно считается задачей руководства компаний, подпадающих под действие NIS2. Кроме того, в NIS2 также обязательны минимальные требования безопасности. Директива регулирует гораздо больше. Но важно помнить, что NIS2 рассматривается европейским законодателем как универсальный. В этом смысле NIS2 можно рассматривать как основу европейских правил кибербезопасности.

DORA устанавливает правила, которым должен соответствовать именно финансовый сектор в сфере кибербезопасности. Как и НИС2, ДОРА также уделяет должное внимание управлению рисками и задачам менеджмента финансовых компаний. Просто потому, что DORA является нормативным актом, его не нужно переносить в национальное законодательство. В то время как это в случае с NIS2.

Если вы хотите узнать больше об обязательствах и возможностях, которые предлагают NIS2 и DORA, пожалуйста, свяжитесь с нами для ознакомительной Ёвстречи.

Обмен информацией и сотрудничество

Перед Национальным центром кибербезопасности (NCSC) и Центром цифрового доверия (DTC) также стоит задача предоставления информации о цифровых угрозах. Короче говоря, NCSC предоставляет эту информацию жизненно важным секторам, а DTC — остальному бизнес-сообществу. В последние годы было

много разговоров о типе информации и способе предоставления информации об угрозах.

7 сентября было объявлено, что цель состоит в том, чтобы к 2026 году иметь единую организацию знаний и информации в области кибербезопасности. До тех пор эти организации также много работают вместе. Потому что, хотя обязательства по кибербезопасности уже применяются, будут применяться или будут расширены для определенных секторов и компаний, компании, на которые эти обязательства не распространяются, также должны иметь дело с цифровыми угрозами.

Управление по телекоммуникациям Нидерландов и AIVD также объявили прошлым летом о сотрудничестве в области кибербезопасности. В частности, в области сертификации ИТ-продуктов и услуг…». ***(Hugo van Aardenne, Jouko Barensen. Cybersecurity – actualiteiten // Ploum (https://ploum.nl/kenniscentrum/nieuws/cybersecurity-actualiteiten). 13.09.2022).***

***

«Европейский Союз должен провести черту между приемлемым использованием хакерских инструментов правоохранительными органами и злонамеренным использованием шпионского ПО для политического и корпоративного шпионажа, а также против журналистов и гражданского общества, заявил в четверг вице-президент блока Маргаритис Схинас.

«Нам нужен некоторый порядок, нам нужна структура, нам нужны судебные гарантии и нам нужен подход ЕС, чтобы положить конец злонамеренному использованию этих продуктов», — сказал Шинас.

Использование хакерских инструментов спровоцировало политические кризисы в Польше, Венгрии, Испании и Греции после того, как стало известно, что деятели политической оппозиции, представители гражданского общества и журналисты стали жертвами хакерского программного обеспечения.

Схинас, гражданин Греции, был назначен в Европейскую комиссию правительством Греции и является членом правящей партии «Новая демократия» премьер-министра Кириакоса Мицотакиса — партии, которая подвергается резкой критике со стороны политической оппозиции и правозащитных групп из-за предполагаемого использования шпионского ПО. органами государственной власти.

Шум от прослушивания в Греции резко усилился 5 августа, когда два высокопоставленных чиновника из правоцентристской администрации премьер-министра Кириакоса Мицотакиса были уволены после того, как выяснилось, что телефон Никоса Андрулакиса, главы левоцентристской партии Пасок, прослушивался. Правительство Мицотакиса признало, что оно действовало неправильно, но заявило, что прослушивание телефонных разговоров было проведено шпионской службой на законных основаниях, хотя до сих пор отказывается говорить почему, ссылаясь на национальную безопасность.

Запутав дело, примерно в то же время была предпринята отдельная попытка взломать телефон Андрулакиса с помощью нелегального программного обеспечения под названием Predator, но Афины категорически отрицают, что их секретные агенты имели какое-либо отношение к этому.

Сама Европейская комиссия также стала жертвой шпионского ПО. Агентство Reuters сообщило в апреле, что комиссар Дидье Рейндерс был среди нескольких высокопоставленных чиновников ЕС, которые стали мишенью шпионского ПО под названием Pegasus, и POLITICO подтвердило, что один из этих чиновников был сотрудником вице-президента Европейской комиссии Веры Юровой.

Европейский парламент создал специальный комитет по расследованию его использования, но Комиссия изо всех сил пыталась принять меры против национальных правительств, которые утверждали, что использование хакерских инструментов подпадает под национальный суверенитет. Тем не менее, в последние годы ЕС принимал законодательные и судебные иски о том, как инструменты наблюдения, такие как хранение данных, используются органами национальной безопасности и как они обеспечивают баланс между конфиденциальностью и безопасностью в таких вопросах, как шифрование.

«У нас нет такой системы для шпионского ПО. И это меня раздражает», — сказал Схинас.

Вице-президент заявил, что необходимо найти «правильный баланс» между необходимостью для спецслужб «преследовать плохих парней» и соблюдением верховенства закона ЕС с точки зрения судебного контроля и защиты данных…». ***(Antoaneta Roussi. Top EU official calls for 'judicial guarantees' to stop abuse of spyware // POLITICO (https://www.politico.eu/article/top-eu-official-call-judicial-guarantee-stop-abuse-spyware/). 15.09.2022).***

***

«За оцінками експертів, найближчими роками Фінляндії знадобиться близько 15 тисяч нових фахівців у сфері кібербезпеки.

Про це повідомляє Yle…

«У Фінляндії спостерігається брак фахівців у сфері кібербезпеки, проте рівень навчання цієї професії не відповідає вимогам робочого життя», - йдеться у публікації.

Це випливає з опитування, проведеного університетом Ювяскюля з метою з'ясувати потреби країни у сфері кібербезпеки.

Згідно з дослідженням, 35% компаній, що працюють у цьому напрямку, вважають гостру нестачу фахівців перешкодою на шляху до зростання та розвитку діяльності.

Як зазначається, Асоціація компаній, які діють у сфері кібербезпеки, заявляє, що найближчими роками Фінляндії (населення якої становить 5,5 мільйона) знадобиться близько 15 тисяч нових фахівців.

На цьому тлі, уточнює видання, торік було збільшено на 300 кількість місць на програмах, які навчають обробці інформації та передачі даних». ***(Фінляндії гостро бракує фахівців з кібербезпеки // Укрінформ (https://www.ukrinform.ua/rubric-technology/3579049-finlandii-gostro-brakue-fahivciv-z-kiberbezpeki.html). 25.09.2022).***

***

«Кибератаки и геополитика угрожают сегодняшнему все более цифровому миру, приводя к нарушению основных поставок, таких как электричество и вода. ЕКА, Европейская комиссия и космические компании в Европе объединяют усилия для создания высоконадежной спутниковой системы связи для ЕС, основанной на нерушимых законах физики.

Спутник Eagle-1 станет первой космической системой распределения квантовых ключей в Европе, которая будет разработана в рамках этого партнерства в рамках контракта, только что согласованного между ESA и SES со штаб-квартирой в Люксембурге при поддержке Европейской комиссии. SES возглавляет консорциум из более чем 20 европейских компаний.

Спутник проложит путь к сверхзащищенной сети, основанной на законах квантовой механики для обеспечения безопасности информации, что значительно повысит автономию Европы в области кибербезопасности и коммуникаций.

Eagle-1 продемонстрирует осуществимость технологии квантового распределения ключей, которая использует принципы квантовой механики для распределения ключей шифрования таким образом, что любая попытка подслушивания будет немедленно обнаружена, в пределах ЕС с использованием спутниковой системы. Для этого система будет основываться на ключевых технологиях, разработанных в рамках программы ESA Scylight, с целью проверки жизненно важных компонентов, поставляемых в ЕС.

Он продемонстрирует и подтвердит технологии передачи квантовых ключей с низкой околоземной орбиты на землю и предоставит ценные данные миссии для разработки и развертывания европейской инфраструктуры квантовой связи (EuroQCI), которая будет интегрирована в европейскую систему безопасной связи. Это позволит ЕС подготовиться к созданию суверенной, автономной трансграничной сети квантово-безопасной связи.

Первоначально система будет использовать модернизированный оптический наземный терминал Немецкого аэрокосмического центра (DLR) вместе с новым оптическим наземным терминалом, который будет разработан командой из Нидерландов. Спутник на платформе Eagle-1 будет эксплуатироваться SES со штаб-квартирой в Люксембурге. Другие государства-члены ЕКА, участвующие в проекте, включают Австрию, Бельгию, Чехию, Италию и Швейцарию.

Спутник Eagle-1 должен быть запущен в 2024 году, после чего пройдет трехлетняя орбитальная проверка при поддержке Европейской комиссии.

Йозеф Ашбахер, генеральный директор ЕКА, сказал: «Европейские космические инновации набрали сильный импульс как с технологической точки зрения, так и с точки зрения коммерциализации. связь, сети следующего поколения и кибербезопасность. Под руководством ESA, частично финансируемого Европейской комиссией и реализуемого SES, Eagle-1 является важным шагом на пути к тому, чтобы сделать реальностью безопасную и масштабируемую европейскую инфраструктуру квантовых коммуникаций».

Элоди Виау, директор по телекоммуникациям и интегрированным приложениям в ESA, сказала: «В сегодняшнем все более взаимосвязанном мире обеспечение безопасности информации имеет первостепенное значение. Надежные ключи шифрования, а также технологии, обеспечивающие их безопасное

распространение, жизненно важны для этого начинания. Мы гордимся тем, что создали это партнерство между ESA и консорциумом во главе с SES для создания высокозащищенной и автономной системы распределения квантовых ключей Eagle-1. ESA позволяет европейской космической отрасли добиться успеха, объединяя промышленность вокруг крупномасштабных программ, добиваясь конкурентных скачков вперед».

Стив Коллар, главный исполнительный директор SES, сказал: «Европейская безопасность и суверенитет в будущем мире квантовых вычислений имеют решающее значение для успеха Европы и ее государств-членов. Мы гордимся тем, что используем наши многоорбитальные возможности и наши инновационные платформы и решения в партнерстве с ЕКА, Европейской комиссией и правительством Люксембурга для продвижения квантовых коммуникаций и разработки системы Eagle-1 для поддержки безопасных и суверенных европейских сетей будущего». ***(Quantum encryption to boost European autonomy // Tech Xplore (https://techxplore.com/news/2022-09-quantum-encryption-boost-european-autonomy.html). 22.09.2022).***

***

Російська Федерація

«Заступник голови правління російського Сбербанку Станіслав Кузнєцов заявив нещодавно під час публічного заходу про те, що в Росії дуже не вистачає експертів у сфері кібербезпеки…

На Східному економічному форумі заступник голови Сбербанку заявив, що фахівців з кібербезпеки у РФ вкрай мало. Він наголосив, що за оцінками Сбербанку, лише 5 тисяч експертів працюють у цій галузі, а необхідно у 20 разів більше (тобто 100 тис.). Також він зазначив, що держава має виправити ситуацію, сформувавши замовлення на кадри.

Видання, посилаючись на главу Російської асоціації електронних комунікацій (РАЕК), пише, що у лютому-березні з Росії виїхали 50-70 тис. айтішників, серед яких, звичайно, були й експерти у сфері кібербезпеки. У РАЕК також вважають, що навесні 2022 могли виїхати ще близько 100 тис. працівників IT. Водночас прем'єр-міністр РФ Мішустін стверджує, що понад 80% айтішників повернулися на територію Росії у травні.

Держава намагається повернути людей, які залишили країну через агресію проти України. Їм пропонують різноманітні пільги — занижені ставки іпотечних кредитів, відстрочення від призову до армії та ін.

Рекрутингова компанія HeadHunter нещодавно провела дослідження і виявилося, що кількість вакансій в IT-галузі у РФ скоротилася. А резюме, навпаки, побільшали на 55%...» ***(Росію нікому захищати в кіберпросторі: у країні залишилося 5 тис. Фахівців // Фокус (https://focus.ua/uk/digital/528213-rossiyu-nekomu-zashchishchat-v-kiberprostranstvi-v-strane-ostalos-5-tys-specialistov). 06.09.2022).***

***

«Исследование Университета Квинсленда выявило необходимость уделять приоритетное внимание обучению директоров советов директоров кибербезопасности, чтобы лучше защитить австралийские организации от кибератак.

Доктор Ивано Бонджованни из бизнес-школы UQ сказал, что его исследование показало, что члены советов директоров не всегда уверены в своих обязанностях и ответственности за кибербезопасность и часто не полностью понимают ее важность.

«Как показала утечка данных в Optus в этом месяце, ни одна организация не застрахована от киберпреступлений», — сказал доктор Бонджованни.

«Мы опросили неисполнительных директоров 43 организаций о кибербезопасности; возникла большая неопределенность с точки зрения современных передовых практик или отраслевых рекомендаций по стратегиям кибербезопасности.

«Существует ошибочное представление о том, что кибербезопасность — это чисто техническая тема, и режиссеры не были заинтересованы или уверенно говорили об этом.

«Учитывая, что ответственность за надзор за управлением киберрисками в современных организациях лежит на их совете директоров, необходимо повышение кибер-навыков на уровне совета директоров».

Сбой кибербезопасности считается одной из главных угроз, с которыми сталкиваются австралийские предприятия, и в связи с доступом к информации о клиентах в результате атаки на Optus Австралийский центр кибербезопасности предупреждает компании, чтобы они оставались начеку.

Соавтор исследования и выпускница UQ с отличием Меган Гейл сказала, что потенциальное влияние утечек данных на австралийские организации было огромным.

«Нарушение ИТ-инфраструктуры может привести к закрытию компании, что приведет к финансовым потерям или даже к более серьезным последствиям», — сказала г-жа Гейл.

«В результате взлома Optus был получен доступ к конфиденциальной личной информации клиентов, а также к документам, удостоверяющим личность, что подвергает людей риску стать жертвами мошенничества».

Исследователи призвали к более четким правилам и методам отчетности, а также к тому, чтобы обучение кибербезопасности стало приоритетом для всех директоров советов директоров.

«Не только советы директоров крупных компаний должны быть лучше оснащены в этой области, — сказала г-жа Гейл.

«Советы малых и средних организаций во всех секторах Австралии, включая некоммерческие и общественные организации, должны быть бдительными».

Директор по кибербезопасности в UQ и австралийской группы реагирования на чрезвычайные ситуации в области кибербезопасности AusCERT доктор Дэвид

Стокдейл сказал, что исследование показало, что Австралии есть над чем поработать, чтобы советы директоров включили кибербезопасность в свою деятельность по управлению корпоративными рисками.

«Как мы видели на Optus, киберугрозы — это вопрос «не если, а когда», и организации должны быть к этому готовы», — сказал доктор Стокдейл.

«Дополнительное обучение киберрискам и регулярное общение между руководителями и их группами безопасности обеспечат наилучший план действий и предотвращения».

В исследовании также принимал участие доцент Сергей Слапникар из бизнес-школы UQ. Их исследование было опубликовано в Computers & Security». ***(Australian board directors urged to boost cybersecurity skills // Tech Xplore (https://techxplore.com/news/2022-09-australian-board-directors-urged-boost.html).*** 27.09.2022).

***

«В этом году в Австралии могут быть приняты новые жесткие законы о защите данных в качестве срочного ответа на кибератаку, в результате которой у телекоммуникационной компании были украдены личные данные 9,8 миллиона клиентов, заявил в четверг генеральный прокурор.

Генеральный прокурор Марк Дрейфус заявил, что правительство проведет «срочные реформы» в Законе о конфиденциальности после беспрецедентного взлома на прошлой неделе Optus, второго по величине оператора мобильной связи Австралии.

Дрейфус сказал: «Я думаю, что это возможно», чтобы закон был изменен в течение оставшихся четырех недель, когда парламент должен заседать в этом году.

«В течение следующих четырех недель я буду очень внимательно изучать, сможем ли мы провести реформы Закона о конфиденциальности в парламенте до конца года», — сказал Дрейфус журналистам. Следующее заседание парламента состоится 25 октября.

Дрейфус сказал, что штрафы за неспособность защитить личные данные должны быть увеличены, чтобы корпоративные советы не могли отклонить штрафы как «расходы на ведение бизнеса».

По словам Дрейфуса, «абсолютно огромные объемы» данных о клиентах, которые компании хранили в течение многих лет, должны быть оправданы в соответствии с измененным законом.

«Компании должны рассматривать хранение данных не как актив, а как пассив или потенциальную ответственность», — сказал Дрейфус. «Слишком долго у нас были компании, рассматривающие данные исключительно как актив, который они могут использовать в коммерческих целях».

Правительство винит в краже личной информации нынешних и бывших клиентов Optus, дочернюю компанию Singapore Telecommunications Ltd., также известную как Singtel, из-за слабой кибербезопасности.

Данные включали паспорт, водительские права и национальные идентификационные номера медицинских учреждений, которые могли быть использованы для кражи личных данных и мошенничества.

Власти критикуют первоначальную неспособность Optus раскрыть, что номера Medicare были среди украденных данных. Это стало очевидным во вторник, когда хакер выложил записи 10 000 клиентов в темную сеть — через шесть дней после того, как Optus обнаружил кибератаку.

Срочный законодательный ответ отделен от более широкого пересмотра Закона о конфиденциальности, который начался три года назад. Закон был принят в 1988 году, и критики утверждают, что его крайне необходимо адаптировать к цифровому веку.

По заявлению правительства, Optus может быть оштрафован на максимальную сумму в 2 миллиона австралийских долларов (1,3 миллиона долларов) за нарушение Закона о конфиденциальности.

Правительство заявило, что за аналогичное нарушение безопасности в соответствии с законами Европейского Союза компания может быть оштрафована на сотни миллионов долларов.

В материалах для обзора Закона о конфиденциальности предлагались штрафы за нарушения, эквивалентные 10% дохода от операций в Австралии.

Генеральный директор Optus Келли Байер Розмарин выступила против увеличения штрафов, заявив во вторник Австралийской радиовещательной корпорации: «Честно говоря, я не уверен, какие штрафы приносят пользу кому-либо».

Optus утверждает, что это была цель изощренной кибератаки, которая проникла через несколько уровней безопасности.

После экстренной встречи с представителями банковского и потребительского надзора министр финансовых услуг Стивен Джонс заявил, что «мошенники» и «мошенники» уже начали использовать украденные данные, в том числе номера телефонов и адреса электронной почты.

С учетом того, что в результате взлома была украдена личная информация 38% 26-миллионного населения Австралии, «нельзя переоценить влияние этого взлома на проблемы потребителей», — сказал Джонс.

Он предостерег скомпрометированных клиентов Optus от активации URL-адресов, которые они получают в текстовом или электронном письме, поскольку они могут быть отправлены преступниками, пытающимися украсть дополнительную информацию.

«Мы все делаем все возможное, чтобы попытаться преодолеть длинный шлейф проблем, которые станут следствием этой масштабной утечки данных», — сказал Джонс». ***(ROD McGUIRK. Australia flags tough new data protection laws this year // Tech Xplore (https://techxplore.com/news/2022-09-australia-flags-tough-laws-year.html). 29.09.2022).***

***

Інші країни

«В августе 2022 года правительство Вьетнама издало Постановление 53/2022 о реализации различных положений Закона о кибербезопасности 2018

года (LCS 2018). Ниже мы резюмируем некоторые ключевые моменты Указа 53/2022:

Локализация данных: Указ 53/2022 содержит более подробные инструкции по локализации данных во Вьетнаме. Пожалуйста, смотрите наш отдельный блог по этому вопросу Здесь.

Использование криптографии («mật mã») для защиты сетевой информации: если это необходимо для национальной безопасности, безопасности и порядка в обществе или для защиты законных прав и выгод других лиц, власти могут потребовать от связанных лиц/организаций зашифровать информацию, не считающуюся государственной тайной. перед хранением, передачей в сети Интернет;

Удаление незаконной или ложной информации в киберпространстве: Информация, подлежащая удалению, включает в себя: среди прочего, информацию о киберпространстве, определенную властями как имеющую содержание, нарушающее национальную безопасность, пропаганду против государства, подстрекающую к насилию, нарушающую безопасность или общественный порядок; основанная на законных основаниях информация, носящая унизительный или клеветнический характер, нарушающая порядок ведения хозяйства, фабрикующая и фальсифицирующая, вводящая в заблуждение людей, наносящая серьезный ущерб социально-экономической деятельности. Процедура применения этой меры включает ключевые этапы, среди прочего, начальник отдела кибербезопасности и профилактики высокотехнологичных преступлений выносит решение о применении данной меры, а затем направляет письменное требование поставщику услуг в сети связи, сети Интернет об удалении соответствующей информации. Это руководство предоставит правительству четкую основу для контроля за распространением непроверенной информации в киберпространстве (например, в социальных сетях, таких как Facebook).

Сбор электронных данных, связанных с противоправными действиями в киберпространстве: – При необходимости для расследования, рассмотрения посягательств на национальную безопасность, общественный порядок и безопасность, права и выгоды других лиц в киберпространстве, начальник отдела кибербезопасности и предотвращения преступлений в сфере высоких технологий примет решение о применении этой меры. Сбор электронных данных должен обеспечивать соблюдение определенных принципов, включая, среди прочего, сохранение статуса цифровых устройств и данных.

Приостановка или прекращение работы информационной системы; изъятие доменных имен: если (i) есть доказательства того, что работа информационной системы нарушает законы о кибербезопасности, национальной безопасности или (ii) информационная система используется для нарушения национальной безопасности, общественного порядка и безопасности, министр Министерство общественной безопасности будет непосредственно определять применение этой меры. В экстренных случаях Департамент кибербезопасности и предотвращения преступлений в сфере высоких технологий может напрямую запросить у соответствующих лиц/организаций приостановку или прекращение работы информационной системы.

Указ 53/2022 устанавливает процедуры проверки кибербезопасности, применимые к информационной системе, не входящей в список информационных систем национальной безопасности.

Указ 53/2022 предусматривает создание и оценку, оценку, проверку и устранение инцидентов информационной системы национальной безопасности». ***(Trinh Phuong Thao, Nguyen Quang. Decree 53/2022 implementing the Law on Cybersecurity in Vietnam // Vietnam Business Law (https://vietnam-business-law.info/blog/2022/9/4/decree-532022-implementing-the-law-on-cybersecurity-in-vietnam). 04.09.2022).***

***

«Тайский национальный комитет по кибербезопасности (NCSC), как того требует Закон о кибербезопасности, в середине августа отчитался перед кабинетом министров о тенденциях и событиях, связанных с киберинцидентами в Таиланде. По данным NCSC, в пятерку наиболее распространенных кибер-инцидентов входят фишинг веб-сайтов, порча веб-сайтов, утечка данных, уязвимости в системе безопасности данных и программы-вымогатели.

За последние годы увеличилось количество зарегистрированных случаев кибератак. В отчете говорится, что затронутые организации в первую очередь реагировали на киберинциденты и атаки, уведомляя NCSC об инциденте и запланированных или предпринятых мерах по исправлению положения, а также проводя внутреннее обучение для повышения осведомленности о киберугрозах. Только две организации решили проводить оценку ИТ-рисков и тесты на уязвимости в качестве превентивных мер против будущих киберугроз.

Отчет NCSC также показал, что помимо операторов телекоммуникационной инфраструктуры, энергетики и коммунальных услуг, а также операторов образования, ставших жертвами кибератак, операторы здравоохранения, веб-хостинга и центров обработки данных также стали «более частыми жертвами» киберинцидентов.

NCSC рекомендовал всем организациям подготовиться к неизбежным киберинцидентам в будущем. Это включает в себя обеспечение того, чтобы предприятия и организации соблюдали международные стандарты, включая меры, признанные и включенные в Закон Таиланда о защите персональных данных (PDPA) и Закон о кибербезопасности.

NCSC также рекомендует проводить внутреннее обучение сотрудников, а также директоров и должностных лиц, поскольку это может помочь предотвратить киберинциденты и обеспечить соблюдение предприятиями минимальных необходимых стандартов безопасности, опубликованных Комитетом по защите персональных данных (PDPC) в его уведомлении Re: Меры безопасности контроллера данных B.E. 2565 (2022), который вступил в силу 21 июня 2022 г. Минимальные требуемые стандарты безопасности для конкретных отраслей (например, те, которые регулируются Банком Таиланда, Управлением страховой комиссии и т. д.) также следует рассматривать в сочетании со стандартами,

указанными в это уведомление PDPC, особенно когда отраслевые требования являются более строгими, чем меры, рекомендованные PDPC.

Законодательные санкции PDPA включают гражданско-правовую ответственность в виде штрафных санкций, административных штрафов и уголовных наказаний, направленных как на предприятия, так и на их директоров и должностных лиц. Однако доказательство того, что эти стороны выполнили применимые требования и внедрили минимальные необходимые стандарты защиты данных, может значительно снизить риск, потенциальную ответственность и штрафы в результате кибератак, особенно инцидентов, связанных с личными данными и конфиденциальными личными данными». ***(Thailand Cybersecurity Report Calls for Organizational Readiness // Tilleke & Gibbins International Ltd. (https://www.tilleke.com/insights/thailand-cybersecurity-report-calls-for-organizational-readiness/). 06.09.2022).***

***

«По мере приближения крайнего срока соблюдения новых руководящих принципов кибербезопасности Индийской группы по компьютерным чрезвычайным ситуациям (CERT-In) микро-, малые и средние предприятия (ММСП) изо всех сил пытаются соблюдать правила.

Новые правила были опубликованы 28 апреля, а позже срок был продлен до 25 сентября.

Правила требуют от компаний сообщать об инцидентах безопасности в течение шести часов после их обнаружения, среди прочего. Они также требуют, чтобы провайдеры виртуальных частных сетей (VPN) отслеживали данные пользователей и предоставляли их правительству по запросу.

По данным отраслевых торговых групп, фирм по кибербезопасности, которые предоставляют инструменты, совместимые с CERT-In, и отраслевых экспертов, общая готовность участников отрасли остается низкой. В четверг Индийский форум МСП написал письмо правительству с просьбой о дальнейшем продлении крайнего срока. Индийский форум МСП — это отраслевая организация, представляющая ММСП.

Новые правила кибербезопасности были изданы в соответствии с подразделом (6) раздела 70B Закона об информационных технологиях 2000 г., который находится в ведении Министерства электроники и информационных технологий (MeitY).

Эксперт по киберправу и юрист Верховного суда Паван Дуггал сказал, что низкий уровень готовности не может быть оправданием для ММСП, и компании в конечном итоге столкнутся с уголовной ответственностью в виде тюремного заключения и штрафов в соответствии со статьей 70B Закона об информационных технологиях за несоблюдение правил. Низкая готовность является одной из главных проблем отраслевых экспертов, которые говорят, что ММСП не готовы соблюдать такие строгие правила, поскольку многие из них никогда серьезно не относились к безопасности. В результате им, вероятно, потребуется еще одно расширение для наращивания мощностей и соблюдения новых правил кибербезопасности. «ММСП в Индии потребуется больше времени, чтобы следовать новым правилам. Им не хватает возможности сообщать об инцидентах и не хватает времени для ее

создания», — сказал Винод Кумар, президент Форума малых и средних предприятий Индии…

Правила также требуют от компаний вести файлы журналов в течение 180 дней и сообщать о любых кибер-инцидентах, определенных в правилах, в течение шести часов. Это потребует «значительных инвестиций» в технологии безопасности и найма специалистов, сказал Алоке Кумар Дани, партнер Deloitte India.

Эксперт по кибербезопасности, пожелавший остаться неназванным, сказал, что минимальные инвестиции для компании с 10 сотрудниками в назначение внешней охранной фирмы могут стоить от 2 до 15 лакхов. Он предупредил, что затраты могут возрасти в зависимости от объема работ, продолжительности контракта и т. д.

Отдельно соучредитель охранной фирмы сказал, что он взимает с малого бизнеса 20 000 фунтов стерлингов за заявку и что это будет стоить не менее 5 лакхов для компании из 30-40 человек.

«Банк, который использует 200 и более приложений одновременно, потратит 40-50 лакхов за годовой контракт. Стоимость также различается в зависимости от типа контракта и т. д.», — сказал он.

В прошлом месяце Mint сообщил, что средняя заработная плата специалистов по безопасности также выросла с августа 2021 года.

Аналитик по безопасности на начальном этапе с опытом работы не менее четырех лет может стоить около 7,5 лакхов в год, в то время как старшие аналитики с десятилетним опытом зарабатывают около 22 лакхов в год...» ***(Sohini Bagchi, Abhijit Ahaskar. MSMEs seek more time to meet CERT-In's cybersecurity rules // HT Digital Streams Ltd (https://www.livemint.com/industry/msmes-seek-more-time-to-meet-cert-in-s-cybersecurity-rules-11663918033947.html). 23.09.2022).***

***

«Стратегия обеспечения кибербезопасности Азербайджана передана в Кабинет министров для утверждения.

Об этом сказал руководитель Государственной службы специальной связи и информационной безопасности Азербайджана Турал Мамедов в ходе мероприятия на тему «Кибербезопасная экономика: реформы, инновационные подходы и решения», передает в среду Trend.

По его словам, старт формированию стратегии кибербезопасности Азербайджана был дан еще в 2018 году.

«Она охватывает такие сферы, как глобальные тренды, цели, анализ текущей ситуации, а также приоритетные направления: кибербезопасность инфраструктура, борьба с мошенничеством и атаками, формирование кибергигиены, международное сотрудничество и ряд других», - сказал он.

Мамедов отметил, что процесс утверждения стратегии затянулся в связи с адаптацией к законодательству, быстрыми изменениями киберсреды и некоторыми другими причинами.

«В настоящее время стратегия представлена в Кабмин для утверждения», - сказал он.

По словам Мамедова, стратегия охватывает и сектор образования и информирования.

«Мы активно сотрудничаем с местными вузами для подготовки программы обучения студентов по соответствующим специальностям. Так, в сотрудничестве нашей госслужбы с одним из вузов страны мы намерены в ближайшие три года обучить бесплатно 1000 ИТ-специалистов»,- сказал он». ***(Садраддин Агджаев. Стратегия обеспечения кибербезопасности Азербайджана представлена в Кабмин для утверждения // АМИ Тренд (https://www.trend.az/business/it/3647104.html). 21.09.2022).***

***

«Ландшафт угроз кибербезопасности развивается так быстро, что сингапурским компаниям сложно за ним успевать. Половина чувствует себя «затопленной» бесконечным потоком кибератак, описывая это как одно из своих самых больших разочарований в работе.

Всего 25 % специалистов по кибербезопасности в Сингапуре были «очень уверены» в способности своей организации адаптироваться к новым угрозам по сравнению со средним показателем в 36 % по всему миру. Еще 62% на азиатском рынке признали, что изо всех сил пытаются не отставать от меняющегося ландшафта угроз, показал опрос, проведенный Coleman Parkes, в котором приняли участие 500 лиц, принимающих решения в области кибербезопасности в Сингапуре. Они были частью глобального исследования, проведенного по заказу поставщика средств безопасности Trellix, в ходе которого были собраны ответы 9000 лиц, принимающих решения в области кибербезопасности, из 15 стран, включая Индию, Индонезию, Австралию, Германию, США и Великобританию.

Респондентам в Сингапуре в среднем приходилось сталкиваться с 54 инцидентами кибербезопасности ежедневно, при этом 39% решали от 50 до 200 таких инцидентов в день. Во всем мире 34 % заявили, что сталкивались с 25–50 инцидентами безопасности в день, а 25 % — в два раза чаще.

В Сингапуре 80% заявили, что нарушения безопасности за последние 12 месяцев привели к потере до 10% дохода их организации. Респонденты из среднего бизнеса с доходом от 50 до 100 миллионов долларов оценили, что их компания потеряла в среднем 9% дохода, в то время как представители крупных предприятий с доходом от 10 до 25 миллиардов долларов заявили, что потери составили в среднем 5% от дохода.

Около 64% заявили, что их нынешние инструменты безопасности не помогают их группе операций по обеспечению безопасности работать с максимальной эффективностью, а 35% признались, что в их защите есть пробелы. Еще 90% заявили, что их инфраструктура кибербезопасности «разрознена».

Около 38 % заявили, что в ближайшие 18 месяцев они, скорее всего, внедрят инструменты сетевого обнаружения и реагирования, 36 % указали на оркестровку безопасности (NDR), автоматизацию и реагирование (SOAR), а 35 % заявили, что внедрят информацию о безопасности и управление событиями. (СИЭМ).

«Разрозненные системы безопасности ложатся ненужным бременем на перегруженные службы безопасности, делая организации легкой мишенью для

злоумышленников», — сказал Джонатан Тан, управляющий директор Trellix в Азии. «Пришло время отказаться от разрозненной безопасности как существующего положения и предпринять конкретные шаги по созданию более гибкой и интеллектуальной модели безопасности, которая в конечном итоге поможет защитить конфиденциальные данные».

Согласно опросу, 45% сотрудников во всем мире назвали ошибки сотрудников, такие как загрузка скомпрометированных файлов или переходы по вредоносным ссылкам, главной угрозой кибербезопасности, с которой столкнулась их организация. Еще 39% указали на внутреннюю угрозу, а 34% назвали фишинг и целевые фишинговые атаки главными угрозами.

Около 30% заявили, что атаки программ-вымогателей, а 29% назвали плохую кибергигиену главной угрозой кибербезопасности, с которой столкнулась их организация.

На вопрос о своих главных проблемах в области кибербезопасности 44 % указали на высокую стоимость продуктов и услуг в области кибербезопасности, 39 % указали на трудности с обнаружением сложных угроз и реагированием на них, а 36 % были обеспокоены отсутствием информации об угрозах и информации об угрозах». ***(Eileen Yu. Singapore firms see 54 cybersecurity incidents daily, struggle to keep up // ZDNET (https://www.zdnet.com/article/singapore-firms-see-54-cybersecurity-incidents-daily-struggle-to-keep-up/). 29.09.2022).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Ціллю кібератаки, що призвела до потрапляння в мережу великого масиву секретних документів Північноатлантичного Альянсу, став Генеральний штаб Збройних сил Португалії.

…про вразливість португальського Генштабу місцевий уряд дізнався лише після отримання повідомлення від США через посольство в Лісабоні.

Ситуацію влада Португалії вважає «вкрай серйозною». Для її вирішення залучені Офіс національної безпеки, а також спецслужби і контррозвідка.

Очікується, що на зустрічі НАТО високого рівня, яка відбудеться наступного тижня, Португалія має надати пояснення, яким чином стався витік інформації. Попередньо було встановлено, що передача секретної інформації відбулася з порушенням протоколів безпеки.

«Ця кібератака була розтягнутою в часі й непомітною: її здійснювали через ботів, запрограмованих виявляти такі документи, які потім у кілька етапів вилучали», – зазначило одне із джерел, що працює в безпекових структурах.

Джерела в португальському уряді, однак, запевняють, що інцидент не вплинув на відносини Португалії та союзників по Альянсу…». ***(Кібератака, через яку в мережу потрапили секретні документи НАТО, була здійснена на Португалію – ЗМІ // Європейська правда (https://www.eurointegration.com.ua/news/2022/09/8/7146443/). 08.09.2022).***

***

«Кража документов НАТО «чрезвычайной важности» у правительства Португалии, по-видимому, была вызвана нарушением протокола безопасности, позволяющим получить доступ через Интернет к файлам, которые должны были быть изолированы. Позже документы были выставлены на продажу на темном веб-сайте.

Сообщается, что таким образом были украдены и предоставлены сотни документов, и португальское правительство сталкивается со сложными вопросами о том, почему утечка не была обнаружена в течение нескольких недель. Инцидент не был обнаружен до тех пор, пока разведка США не наткнулась на украденные документы НАТО в даркнете.

Документы НАТО, украденные без ведома Португалии, не обнаружены до тех пор, пока не будут выставлены на продажу

Документы НАТО были взяты из агентства Генерального штаба вооруженных сил Португалии (EMGFA), правительственного органа, который, по сути, управляет вооруженными силами страны. Считается, что взлом произошел где-то летом, но его еще не обнаружили, поскольку EMGFA совершенно не знала об этом, пока документы не появились в даркнете.

Документы НАТО не были обнаружены разведкой США до тех пор, пока они не были проданы на аукционе в даркнете. Агенты уведомили посольство США в Лиссабоне, которое, в свою очередь, уведомило правительство Португалии, которое распорядилось провести полную проверку сети EMGFA национальным центром кибербезопасности и Управлением национальной безопасности (GNS).

Внутренние источники сообщили местным португальским СМИ, что украденные документы НАТО имели «чрезвычайную серьезность». Это тип документов, которые по протоколу должны храниться в изолированных системах, но источники говорят, что боты, запрограммированные на сканирование таких документов, получили их через Интернет. Сообщается, что атака велась в течение длительного периода времени и в несколько этапов. Правительство Португалии еще не прокомментировало нападение или эти сообщения СМИ.

Если верить сообщениям, наиболее вероятной причиной является то, что кто-то для удобства подключил системы с воздушным зазором к подключенной к Интернету части внутренней сети.

Инцидент поднимает новые вопросы о готовности партнеров НАТО к кибербезопасности вскоре после того, как августовский взлом французской ракетной системы MBDA привел к краже секретных разведывательных документов и их продаже в даркнете. MBDA производит ракеты, которые поставляются НАТО и в настоящее время используются в войне на Украине. В сообщениях указывается, что внешний жесткий диск, принадлежащий одному из поставщиков MBDA, был взломан; 80 ГБ документов всплыли на темном веб-форуме и были проданы как минимум одному покупателю по цене 15 биткойнов. Это нарушение, по-видимому, включало документы НАТО с грифом «секретно» и «секретно», но не носило гриф «высшая космическая тайна». Образец файлов показал, что они были созданы с 2017 по 2020 год.

Сообщается, что документы НАТО также были частью широкомасштабной утечки данных федерального правительства США в 2020 году, которая произошла через технологических партнеров, таких как Microsoft и SolarWinds. Эта атака была приписана поддерживаемым государством передовым группам постоянных угроз России, которые ищут разведывательные данные, а не криминальные спекуляции из даркнета. Участие этих относительно менее опытных групп, которые ранее избегали атак на влиятельные правительственные объекты, чтобы не привлекать к себе слишком много внимания правоохранительных органов, вызывает обеспокоенность.

Преступники становятся все более наглыми: группа вымогателей Conti угрожает «свергнуть» правительство Коста-Рики во время недавней атаки.

Салли Винсент, старший инженер по исследованию угроз в LogRhythm, отмечает, что в последнее время произошла серия небольших атак такого рода, которые демонстрируют, что киберпреступники перестают бояться репрессалий со стороны правительства и видят деньги в краже секретов, в которых раньше были заинтересованы только передовые группы постоянной угрозы национального государства: «Атака на EMGFA следует за другими недавними атаками на правительственные организации. Только в прошлом месяце Instituto Agriculturo Доминиканской Республики и аргентинская судебная власть Кордовы подверглись аналогичным атакам программ-вымогателей — к сожалению, обилие конфиденциальной информации государственных органов делает их привлекательными мишенями для киберпреступников, и эта атака на EMGFA имеет ужасные последствия. Разоблачение национальных государственных секретов в даркнете не только ставит под угрозу военный авторитет Португалии, но и подрывает безопасность НАТО. Якобы, Кибератака произошла после того, как EMGFA нарушила правила операционной безопасности. Чтобы предотвратить подобную атаку, организации должны разработать надежные правила для своих протоколов кибербезопасности и придерживаться их. Кроме того, организации должны всегда помнить о своих технологиях предотвращения и обнаружения, обеспечивать наличие соответствующих средств защиты и следить за тем, что происходит в их среде»… ***(Scott Ikeda. NATO Documents Stolen in Breach of Portuguese Armed Forces, Found for Sale on Dark Web // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/nato-documents-stolen-in-breach-of-portuguese-armed-forces-found-for-sale-on-dark-web/). 15.09.2022).***

***

Чорногорія отримує підтримку від США та інших союзників по блоку НАТО у відбитті кібератак на її інформаційні системи та електронні сервіси, за якими, ймовірно, стоїть росія…

Як заявив міністр державного управління Чорногорії Мараш Дукай, хакери атакували вебсайти та бази даних країни за допомогою програми-вимагача Cuba та нового вірусу під назвою Zero Date. За його словами, більшість державних вебсайтів тимчасово відключено як запобіжний захід.

«Чорногорія не самотня в цій ситуації, наші партнери по НАТО з нами», - додав Дукай.

Міністр внутрішніх справ Чорногорії Філіп Аджич після зустрічі з представниками ФБР у США заявив, що група швидкого реагування ФБР у Чорногорії допоможе впоратися з кібератаками.

«Це є ще одним доказом чудової співпраці між Сполученими Штатами Америки та Чорногорією», - зазначив він.

Очільник відділу кібербезпеки Чорногорії Душан Полович заявив, що особисті дані громадян не потрапили до рук кіберзлочинців. І хоча він прямо не назвав рф винуватцем кібератак, однак державний мовник Чорногорії RTCG, посилаючись на джерела в агенції безпеки країни, заявив, що за нападом стоїть росія, що спонукало уряд Чорногорії звернутися по захист до США та інших союзників по НАТО.

російська федерація неодноразово намагалася дестабілізувати внутрішньополітичну ситуацію в Чорногорії. В 2016 році, за рік до свого вступу до НАТО, Чорногорія запобігла спробі державного перевороту, до якої була причетна росія…». ***(Чорногорію атакували російські хакери - НАТО допомагає їх нейтралізувати // Укрінформ (https://www.ukrinform.ua/rubric-technology/3562720-cornogoriu-atakuvali-rosijski-hakeri-nato-dopomagae-ih-nejtralizuvati.html). 01.09.2022).***

***

«В Організації договору про колективну безпеку (ОДКБ) заявили, що їхній офіційний сайт 13 вересня зазнав DDOS-атаки.

…про це заявила пресслужба ОДКБ у Телеграм-каналі.

«13 вересня близько 23.00 піддався DDOS-атаці офіційний сайт ОДКБ. Була порушена працездатність ресурсу, зафіксовані несанкціоновані спроби внесення змін до деяких інформаційних повідомлень, до 7.00 14 вересня 2022 р. доступ був неможливий», - йдеться у повідомленні.

Наголошується, що наразі працездатність сайту частково відновлена, ведуться заходи щодо локалізації несанкціонованого втручання та відновлення пошкоджених чи втрачених даних…». ***(Хакери зламали сайт ОДКБ // Укрінформ (https://www.ukrinform.ua/rubric-world/3571325-hakeri-zlamali-sajt-odkb.html). 14.09.2022).***

***

«Прем'єр-міністр Еді Рама заявив, що Албанія розриває дипломатичні зв'язки з Іраном після кібератаки на національний портал державних послуг…

«Про це рішення (про розрив дипломатичних зв'язків – ред.) було вказано в офіційній ноті посольству Ірану. Впродовж 24 годин всі дипломати й адміністративний персонал, включаючи охоронців, повинні залишити територію Албанії», - заявив Рама.

За його словами, таке рішення було небажаним, проте повністю відповідає серйозності й небезпечності кібератаки, яка загрожувала «покласти» державні послуги, видалити системи та вкрасти дані.

Рама зазначив, що кібератака на національний портал державних послуг, яка сталася ще 15 липня, була профінансована Іраном.

«Кібератака провалилася, а збитки можна вважати незначними. Співпраця різних інституцій доказала, що кібератака була профінансована Іраном», - додав глава уряду…» ***(Албанія розриває дипломатичні зв'язки з Іраном після кібератаки // Укрінформ (https://www.ukrinform.ua/rubric-world/3566384-albania-rozrivae-diplomaticni-zvazki-z-iranom-pisla-kiberataki.html). 07.09.2022).***

***

«В среду несколько федеральных агентств объявили о новых действиях против граждан Ирана, утверждая, что хакеры атаковали критически важную инфраструктуру американских и глобальных цифровых сетей при поддержке иностранного правительства.

В рамках совместных действий Министерства юстиции, Государственного департамента, Федерального бюро расследований, Киберкомандования США, Агентства национальной безопасности и Агентства по кибербезопасности и безопасности инфраструктуры злоумышленники, идентифицированные как связанные с Корпусом стражей исламской революции Ирана, были подвергнуты санкциям со стороны Управление по контролю за иностранными активами Министерства финансов 14 сентября.

В тот же день Министерство юстиции обнародовало обвинительное заключение против трех из 10 лиц, попавших под санкции. Должностные лица юстиции опознали трех обвиняемых хакеров как Мансура Ахмади, известного как Мансур Ахмади; Ахмад Хатиби Агда, известный как Ахмад Хатиби; и Амир Хоссейн Никаин Равари, также известный под псевдонимами Амир Хоссейн Никаин, Амир Хоссейн Никаин и Амир Никаин. Согласно обвинительному заключению, эти трое, как известно, используют уязвимости в таких приложениях, как Microsoft Exchange и Log4j VMWare Horizon, а также участвуют в операциях по вымогательству.

«ФБР остается непоколебимым в нашей приверженности работе с нашими партнерами из правительства США с целью возложения ответственности на наших противников», — сказал помощник директора киберотдела ФБР Брайан Ворндран. «Это обвинение в сочетании с другими подрывными оперативными действиями демонстрирует, что возможно, когда мы объединяемся с нашими внутренними и международными партнерами и применяем общегосударственный подход. Мы вместе с нашими партнерами по-прежнему привержены защите Соединенных Штатов Америки и жертв, пострадавших от этих вопиющих преступлений».

Чиновники юстиции утверждают, что трое хакеров атаковали цифровые сети организаций, расположенных в Нью-Джерси в период с 2021 по 2022 год. Другие штаты, которые были зарегистрированы в качестве целей для взлома программ-вымогателей, включают Миссисипи, Вашингтон и Вайоминг, где находятся такие учреждения, как приюты для жертв домашнего насилия, строительные компании и государственные учреждения. жилищные корпорации пострадали от утечки данных.

Официальные лица отметили, что предполагаемые хакеры, в частности Хатиби, потребовали выкуп в криптовалюте на сумму 50 000 долларов.

Некоторые из формальных обвинений, предъявленных трем подсудимым, включают сговор с целью компьютерного мошенничества и связанную с ним деятельность, связанную с компьютерами, умышленное повреждение защищенного

компьютера и передачу требования в отношении повреждения защищенного компьютера.

Несмотря на то, что трое обвиняемых находятся на свободе за границей, Министерство финансов наложило санкции в общей сложности на десять хакеров IRCG, в том числе названных Министерством юстиции, и на две организации за их роль в злонамеренных кибератаках, ссылаясь на действия этих организаций как внутри страны, так и за рубежом.

«Актеры-вымогатели и другие киберпреступники, независимо от их национального происхождения или базы операций, нацелились на предприятия и критически важную инфраструктуру по всем направлениям, что напрямую угрожает физической безопасности и экономике Соединенных Штатов и других стран», — сказал заместитель министра финансов США. Терроризм и финансовая разведка Брайан Нельсон в пресс-релизе. «Мы продолжим координировать действия с нашими глобальными партнерами для борьбы и предотвращения угроз программ-вымогателей, в том числе связанных с КСИР».

Помимо отдельных субъектов, Министерство финансов наложило санкции на компании Najee Technology и Afkar System после получения доказательств их участия в атаках на критически важные сети инфраструктуры и использовании распространенных уязвимостей для кампаний программ-вымогателей.

Представители министерства финансов отметили, что помимо нападений на критически важную инфраструктуру, подсанкционные организации также преследовали оборонный и правительственный персонал США и Ближнего Востока. До 10 миллионов долларов предлагается в качестве вознаграждения за информацию, ведущую к местонахождению лиц, находящихся под санкциями, в рамках программы «Награды за правосудие» Государственного департамента.

CISA подчеркнула уведомления Министерства юстиции и Министерства финансов, выявив злоумышленников, действующих под управлением иранских компаний Najee Technology и Hooshmand Fater LLC, в информационном бюллетене, опубликованном в среду. Чиновники CISA подтвердили связь выявленных хакеров с правительством Ирана и КСИР, а также рассказали о программных инструментах и тактиках, используемых этими акторами, таких как BitLocker, для шифрования украденных данных.

«С тех пор как об этой деятельности стало известно в 2021 году, эти аффилированные с КСИР субъекты продолжали использовать известные уязвимости для первоначального доступа», — говорится в бюллетене. «Субъекты могут продавать данные или использовать удаленные данные в операциях по вымогательству или операциях по вымогательству «двойного вымогательства», когда субъект угрозы использует комбинацию шифрования и кражи данных, чтобы заставить целевые организации заплатить требования о выкупе».

Руководство частного сектора подчеркнуло серьезность хакерских атак на критически важные инфраструктурные сети — проблема, которая в последние несколько лет набирает обороты в США.

Николь Дарден Форд, вице-президент по глобальной безопасности и директору по информационной безопасности в Rockwell Automation, сообщила

Nextgov, что основные услуги, такие как очистка воды, находятся под угрозой, поскольку хакеры запускают вредоносные кампании в надежде на крупную выплату.

«Кибервойна со стороны государства представляет серьезную угрозу для нашей критически важной инфраструктуры, на которую мы все полагаемся», — сказала она. «Компании, работающие в этой сфере, должны взять на себя ведущую роль в защите систем от этих атак, чтобы избежать потенциально катастрофических последствий». ***(Alexandra Kelley. Whole-of-Government Effort Targets Iranian Hackers // Nextgov (https://www.nextgov.com/cybersecurity/2022/09/whole-government-effort-targets-iranian-hackers/377230/). 15.09.2022).***

***

«Центр киберпреступности Министерства обороны США (DC3), Управление по поддержке операций (OED) и Киберкомандование США (USCC) участвуют в межведомственном сотрудничестве для активизации усилий по поддержке вопросов национальной безопасности в связи с информацией о киберугрозах.

DC3 предоставляет военному персоналу Cyber National Mission Force (CNMF) ротационные программные задания, связанные с кибераналитиками DC3, расширяя их опыт за счет связи с разведкой киберугроз и анализом вредоносных программ, в то же время предоставляя USCC, заинтересованным сторонам DC3 и разведывательному сообществу критически важную информацию.

«Руководство CNMF и DC3 признало, что эти усилия, безусловно, улучшают сотрудничество и координацию совместных миссий в борьбе со злонамеренными кибер-кампаниями», — сказала Дайана Кинкер, директор OED. «Руководство OED также рассматривает эту инициативу как возможность интеграции CNMF и USCC с услугами и возможностями DC3 и OED».

В июне в DC3 прошел первый семинар по обратному инжинирингу вредоносных программ. Аналитики из DC3, USCC и зарубежных партнеров приняли участие в этом новаторском мероприятии. Мероприятие стало отличной площадкой для аналитиков, которые поработали над сложными образцами вредоносных программ и обменялись передовым опытом и информацией для борьбы с хитростью злоумышленников в киберпространстве.

«Эти постоянные усилия открывают для DC3 возможность делиться киберзнаниями и расширять более широкий опыт в области разведки киберугроз в целях создания отчетов о киберинцидентах, киберрасследований и анализа вредоносных программ», — сказала Пегги Райт, руководитель OED.

«Сотрудничество между DC3 и Киберкомандованием США ясно демонстрирует важность межведомственной оперативности и связанного с этим взаимодействия», — сказал Джошуа Блэк, заместитель директора DC3. «Существует множество агентств и команд, работающих над защитой информационных сетей и систем Министерства обороны, и средства защиты Министерства обороны от киберугроз неизбежно увеличиваются при взаимодействии единомышленников». ***(DoD Cyber Crime Center, U.S. Cyber Command Develop Interagency Collaboration // Homeland Security Today (https://www.hstoday.us/subject-matter-***

areas/cybersecurity/dod-cyber-crime-center-u-s-cyber-command-develop-interagency-collaboration/). 16.09.2022).

***

«Июльская кибератака, приписываемая Ирану, вынудила Албанию разорвать все дипломатические отношения с этой страной, создав то, что Совет национальной безопасности Белого дома называет «тревожным прецедентом для киберпространства».

Это первый случай, когда страна разорвала дипломатические отношения из-за кибератаки. Инцидент 15 июля повредил критически важную инфраструктуру в Албании и закрыл несколько правительственных веб-сайтов, что привело к призыву о помощи к партнерам по НАТО. Иранские дипломаты были выдворены из страны, а посольство закрыто, а албанская полиция обнаружила там лишь документы, сожженные в бочке после того, как уехал последний персонал.

Албания отказывается от дипломатических отношений с Ираном после серьезной кибератаки

Премьер-министр Эди Рама разорвал дипломатические отношения с Ираном в видеообращении 7 сентября, сославшись на июльскую кибератаку и потребовав от сотрудников посольства страны покинуть страну в течение 24 часов. Рама признал, что это был «крайний ответ», но сказал, что это было необходимо, учитывая нанесенный ущерб (и дополнительный риск) государственным службам и государственным документам.

Это объявление последовало за недельным расследованием, проведенным Соединенными Штатами, которое установило, что за кибератакой стоят четыре группы угроз, нанятые иранским правительством. Фирма по кибербезопасности Mandiant отметила, что кампания была в первую очередь нацелена на иранских диссидентов, бежавших в страну, и включала в себя удаление вредоносных данных, а не кражу. Предполагается, что в атаке участвовала модифицированная версия программы-вымогателя, предназначенная для нанесения ущерба, которая могла распространиться за пределы намеченных целей.

Конфликт восходит к 2014 году, когда члены Народной организации моджахедов Ирана, крупнейшей оппозиционной политической группы в стране, были сосланы, а около 3000 человек получили разрешение поселиться в Албании. Ранее Албания разорвала дипломатические отношения в 2018 году, выслав посла на фоне обвинений в подготовке терактов во время отборочного матча чемпионата мира по футболу. С тех пор Иран постоянно подразумевал, что Албания работала против него в направлении смены режима под давлением США и Израиля.

Со своей стороны, Иран отрицает ответственность за кибератаку, несмотря на сообщения ФБР и службы безопасности Microsoft об обратном. Албания официально присоединилась к НАТО в 2009 году, но является частью Совета евроатлантического партнерства с момента его первого создания в начале 1990-х годов и поддерживает дипломатические отношения с США вскоре после создания демократического правительства.

Мандиант сказал, что кибератака была в первую очередь направлена на диссидентов в Албании, а правительство Албании заявило, что оно поймало

иранских агентов, которые ранее предпринимали несколько попыток против диссидентов. Американские следователи, направленные в страну, назвали кибератаку «безрассудной и безответственной», а также «беспрецедентной» из-за ущерба, нанесенного критически важной инфраструктуре в период мирного времени между странами.

Кибератака наносит ущерб госуслугам

В результате атаки были закрыты несколько правительственных веб-сайтов, и Албания утверждает, что хакеры пытались взломать государственные службы, но все было восстановлено и безвозвратной потери данных не произошло. Совет национальной безопасности США добавил, что впоследствии были проведены «операции по взлому и утечке». Это, по-видимому, включало распространение сканов разрешений на проживание диссидентов на канале Telegram, а также обнаружение программы-вымогателя, которая содержала сообщение о том, что диссиденты преследуются.

Правительство Албании заявило, что кибератака имеет сходство с другими инцидентами с участием членов НАТО в прошлом году; к ним относятся Бельгия, Германия, Литва и Нидерланды. Одна из групп, которую Иран, как сообщается, нанял для атаки, была связана с предыдущими атаками на Израиль, Саудовскую Аравию, Объединенные Арабские Эмираты и ряд других стран Ближнего Востока.

Помимо нанесенного ущерба, нападение вынудило диссидентов отменить запланированный Всемирный саммит свободного Ирана, который должен был состояться в Манезе в июле и на котором должны были присутствовать законодатели США. США решительно осудили нападение. Между США и Ираном существует давняя неразрешенная напряженность, но ситуация обострилась в 2019 году с наращиванием военного присутствия США в Персидском заливе после того, как Иран предположительно повредил несколько торговых судов, и снова в 2020 году с точечным ударом по военному командиру Касему Сулеймани, за которым последовал Ракетный удар Ирана по иракским базам, где дислоцированы американские войска. США ввели новые санкции против Ирана, и летом 2021 года произошло еще одно нападение на торговые суда.

Mandiant сообщил, что Иран, вероятно, попытается сорвать предстоящие промежуточные выборы в США или вмешаться в них. Иран обвиняют в попытке вмешательства в выборы 2020 года, а президент Джо Байден ранее заявлял, что страна должна «заплатить цену» за эти попытки. Две страны не имели официальных дипломатических отношений с 1980 года.

Технический анализ кибератаки, проведенный Mandiant, показал, что вместе с программами-вымогателями из семейства Roadsweep были развернуты новая вредоносная программа для стирания данных (вариант «Zeroclear») и новая форма вредоносного ПО («Chimneysweep»)». ***(Scott Ikeda. Albania Drops Diplomatic Ties With Iran in First-Ever Severance of Relations Due to a Cyber Attack // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/albania-drops-diplomatic-ties-with-iran-in-first-ever-severance-of-relations-due-to-a-cyber-attack/). 13.09.2022).***

***

«Кибератака, совершенная подозреваемыми российскими хакерами, нарушила работу не менее 20 правительственных веб-сайтов четырех министерств Японии, включая порталы eLTAX и e-Gov.

Главный секретарь кабинета министров Хирокадзу Мацуно заявил, что ответственность за атаку на правительственные сайты взяла на себя пророссийская группа Killnet.

«Нам известно, что хакерская группа (Killnet) предположила, что она стояла за атаками, но на данный момент мы все еще расследуем причины сбоев, включая причастность этой группы», — сказал Мацуно.

Тем временем в социальных сетях появилось заявление Killnet, в котором говорилось, что группа сопротивлялась милитаризму японского правительства и пинала самураев.

Российские хакеры проводят DDoS-атаки на «вражеские» правительственные сайты

Пророссийская группа хактивистов использует распределенные атаки типа «отказ в обслуживании» (DDoS), чтобы парализовать правительственные веб-сайты враждебных Кремлю стран.

DDoS-атаки включают в себя бомбардировку целевого веб-сайта или сети множеством автоматических запросов, нарушающих ее пропускную способность, что препятствует доступу законных пользователей к веб-сайту.

Российские хакеры осуществили DDoS-атаки на многочисленные правительственные веб-сайты стран, которые поддерживали Украину во время продолжающегося конфликта.

В августе 2022 года та же группа российских хакеров атаковала более 200 эстонских правительственных веб-сайтов после того, как страна убрала советский танк Т-34 из публичной экспозиции в музей.

В мае итальянская группа реагирования на инциденты компьютерной безопасности (CSIRT) заблокировала кибератаку на систему голосования на Евровидении. Кибератака была направлена на то, чтобы помешать Украине выиграть конкурс после того, как организаторы впервые с 1994 года запретили Россию. После атаки CSIRT предупредила о возможных атаках на итальянские предприятия со стороны неназванных российских хакеров, вероятно, группы Killnet.

С января группа заявила о нескольких атаках на территории Японии, в том числе о кибератаке на японскую компанию, выпускающую кредитные карты, и на оператора социальных сетей Mixi.

Российские хакеры не скомпрометировали личную информацию во время кибератаки

Правительственный веб-сайт электронного правительства стал недоступен во вторник, 7 сентября, в 16:30, но к концу дня был восстановлен. Сайт позволяет гражданам подавать заявки на получение различных государственных услуг, знакомиться с законодательством и оставлять отзывы по различным вопросам.

По словам представителей цифрового агентства, кибератака не скомпрометировала личную информацию, хранящуюся на пострадавших веб-сайтах.

Кибератака в ответ на более широкий конфликт

Помимо поддержки Японией Украины в продолжающемся конфликте, две страны враждуют из-за спорных Курильских островов в Тихом океане.

Япония выступила против недавних российских военных учений на оспариваемой территории. Впоследствии Москва отреагировала отказом от безвизового въезда японских граждан на плавучие массивы суши, аннексированные Советским Союзом в конце Второй мировой войны.

Кроме того, Япония также критиковала российское вторжение и участвовала в санкциях против Москвы и помощи Украине.

Таким образом, последняя кибератака может также свидетельствовать о том, что российские хакеры активно нацелены на Японию в продолжающейся более широкой геополитической войне между западными державами, их союзниками и Россией.

«Эта атака на Японию произошла после недавней широкомасштабной атаки Killnet на сайты в Италии, Литве, Эстонии, Польше и Норвегии, и в будущем можно ожидать новых запланированных атак», — сказал Сергей Шикевич, менеджер группы анализа угроз в Check Point. Программное обеспечение.

«Наш недавний полугодовой отчет по безопасности показал, что, помимо глобального роста кибератак на 42%, также произошло огромное увеличение спонсируемых и мобилизованных государством хакерских групп, которые набрали силу с начала российско-украинской войны.»

По словам Надира Израэля, соучредителя и технического директора Armis, кибервойна достигла своего пика, и такие атаки были направлены на то, чтобы раздражать рядовых граждан, заставляя их задаваться вопросом, «почему существуют санкции или почему одно национальное государство вмешивается в конфликты другого».

«Мы наблюдаем резкое изменение смелости: раньше кибервойна пряталась за плащами и кинжалами, проводилась незаметно для радаров исключительно с целью сбора разведывательных данных», — сказал Израэль.

«Сегодня этот наступательный маршрут открыт — возможно, его выставляют напоказ субъекты угроз и национальные государства, стремящиеся вызвать сбои или ущерб».

Израэль отметил, что ландшафт кибервойн значительно изменился за последние пять лет. Однако рядовой гражданин не привык к тому, что кибервойна является законным инструментом, используемым противниками и ставящим всех на передовую. Такие атаки обычно нацелены на правительственные веб-сайты, которые необходимы большинству людей для критически важных услуг, чтобы вызвать разочарование и угрожать общественному порядку.

«Даже если сам сбой не кажется серьезным, кибератака на правительство может вызвать у граждан страх перед хаосом», — предупредил он. «Каждая страна и организация должны очень тщательно продумать свою позицию в области кибербезопасности». ***(Alicia Hope. Cyber Attack by Russian Hackers Disrupted 20 Japanese Government Websites // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/cyber-attack-by-russian-hackers-disrupted-20-japanese-government-websites/). 15.09.2022).***

***

«Уряд Японії перевіряє, хто несе відповідальність за труднощі з доступом до понад 20 вебсайтів у чотирьох міністерствах, що були спричинені атакою типу «відмова в обслуговуванні» (DDoS). Про це повідомляє Reuters.

«Ми знаємо, що група хакерів Killnet заявила, що вона стоїть за атаками, але на цей час ми все ще розслідуємо причини збоїв, включаючи причетність групи», — повідомив головний секретар уряду Хірокадзу Мацуно.

У вівторок ввечері доступу до урядових вебсайтів не було. Проблеми із доступом розв'язали у той же день, додав Мацуно.

Пізніше цифрове агентство Японії повідомило в Twitter, що в середу на його адміністративному порталі e-Gov виникли проблеми із доступом до деяких сервісів. За даними громадського мовника NHK, у вівторок цей портал був одним із тих, хто зазнав хакерської атаки…» ***(Російські хакери атакували Японію за підтримку України // MediaSapiens (https://ms.detector.media/kiberbezpeka/post/30203/2022-09-07-rosiyski-khakery-atakuvaly-yaponiyu-za-pidtrymku-ukrainy/). 07.09.2022).***

***

«Китайское правительство утверждает, что Агентство национальной безопасности (АНБ) стоит за неоднократными нападениями на Северо-Западный политехнический университет, университет аэрокосмических и космических исследований, финансируемый Пекином. Это заявление было сделано после того, как правительство США выпустило предупреждения о том, что поддерживаемые государством группы продвинутых постоянных угроз (APT) Китая «обыскивают» компании в поисках конфиденциальной информации, которая может быть использована для кражи и копирования интеллектуальной собственности.

Китай утверждает, что Управление операций специализированного доступа (TAO) АНБ несет ответственность за десятки тысяч «злобных» кибератак и за последние годы украло более 140 ГБ данных из страны в рамках операций кибершпионажа. Китайский национальный центр реагирования на компьютерные вирусы (NCVERC) утверждает, что провел расследование совместно с Qihoo 360 (китайской компанией, занимающейся интернет-безопасностью), в результате которого были получены доказательства причастности TAO.

Китай и США обвиняют друг друга в кибершпионаже

В течение десятилетий США быстро обвинили китайские хакерские группы APT, когда они считают, что есть доказательства, но Китай, как правило, просто отрицал или игнорировал эти утверждения без встречных обвинений. Но Пекин в последнее время стал более агрессивно называть правительственные учреждения США в инцидентах кибершпионажа, поскольку США все активнее говорят о деятельности Китая в краже интеллектуальной собственности у западных организаций.

Правительство США признало, что иногда занимается кибершпионажем в целях национальной безопасности, но проводит различие между этим и тем, что оно называет «разграблением» исследовательских институтов и частных компаний китайскими хакерами, поддерживаемыми государством. В феврале Китай указал пальцем на еще одну предполагаемую спонсируемую государством хакерскую

группу США; команда под названием «Equation», которая была связана с АНБ, которое, по ее утверждению, взламывало различные ИТ-системы и внедряло вредоносное ПО.

Недавние обвинения Китая также включали кибершпионаж со стороны американских агентств против местного населения страны посредством перехваченных текстовых сообщений, в том числе широкомасштабные утечки Сноудена в 2013 году. Проживая в Гонконге, когда бушевали разногласия по поводу его первоначальных заявлений, Сноуден представил властям документы с подробным описанием программы, которая включала массовый взлом АНБ китайских телефонных компаний для неизбирательного сбора SMS-сообщений. Нынешние заявления также отражают обвинения Сноудена в том, что АНБ взломало Университет Цинхуа, в котором размещался цифровой центр, обеспечивающий доступ к личным данным миллионов граждан Китая.

В случае с атакой на исследовательский университет китайское правительство утверждает, что TAO нацелился на управление сетью и основные технологии с помощью 41 инструмента атаки. Власти не уточнили, чем занимались предполагаемые хакеры, но исследовательский университет известен разработкой ракетных технологий и беспилотников. Он также находится в «списке организаций», запрещающих гражданам США вести с ним дела после того, как гражданин Китая, проживающий в Массачусетсе, был пойман на незаконном экспорте ему деталей, используемых для обнаружения подводных лодок.

Qihoo 360 ранее заявляла, что ЦРУ может быть связано с операциями кибершпионажа в стране с помощью кода, опубликованного Wikileaks, и что эти операции датируются как минимум 2008 годом. В случае атаки на исследовательский университет Китай утверждает, что АНБ использовало ранее неизвестный метод «нулевого дня», чтобы получить первоначальный доступ.

Заявления о нападениях на исследовательский университет могут иметь несколько мотивов

Ни для кого не секрет, что исследовательский университет может стать мишенью для нескольких иностранных государств (а иногда и союзников), и что США являются такой же частью этого международного кибершпионажа, как и все остальные. Заявления Китая, по-видимому, являются прямым ответом на недавнюю риторику США, но также могут включать Qihoo 360 как средство косвенной рекламы своих услуг другим странам, в которых Китай укрепляет свою экономическую позицию.

NCVERC следил за инцидентом в исследовательском университете, заявляя, что у АНБ есть инструменты, способные взломать среды x86 и Sun Solaris, которые используют кремний SPARC, и активно использует их в течение некоторого времени. Подобные заявления также могут быть направлены на то, чтобы посеять сомнения среди других народов.

Джош Лоспиносо, генеральный директор и соучредитель Shift5, рассматривает все это как еще одну часть продолжающейся игры между двумя странами: «Китай в течение многих лет указывал пальцем на Соединенные Штаты в ответ на то, что наше разведывательное сообщество выявляло китайских участников угроз за многочисленные атаки, такие как прошлогодняя атака против Microsoft Exchange..

Публичное обвинение ТАО АНБ во взломе авиационного университета, финансируемого Пекином, безусловно, является стратегическим шагом для Китая в попытке уменьшить мнение о США в соседних странах, таких как Япония и Южная Корея, особенно в свете обострения напряженности после визита Нэнси Пелоси на Тайвань. Этот тип усиления риторики недалек от того, что мы видели со стороны России перед вторжением в Украину, и мне интересно посмотреть, использует ли Китай это как метод смягчения своих целей».

Некоторые наблюдатели также отметили, что сроки этих обвинений в кибершпионаже несколько подозрительны, учитывая, что они выдвигаются как раз перед ежегодной Неделей кибербезопасности в стране. Это мероприятие проводится в начале октября и призвано привлечь внимание общественности к вопросам кибербезопасности и активной защиты. Недавно Китай провел кампанию по партнерству со странами южной части Тихого океана в области защиты от кибербезопасности, вовлекая 10 из них в переговоры в начале этого года. «Цифровой Шелковый путь» также является ключевой частью текущей инициативы страны «Один пояс, один путь», направленной на создание инфраструктуры в самых разных странах, к которым он имеет хотя бы некоторую степень доступа». ***(Scott Ikeda. China Accuses NSA of Cyber Espionage in Repeated Breaches of Xi'an Research University // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/china-accuses-nsa-of-cyber-espionage-in-repeated-breaches-of-xian-research-university/). 19.06.2022).***

***

«Разношерстная группа российских хактивистов нацелена на европейские правительства, инфраструктуру и даже на престижный песенный конкурс «Евровидение» с помощью кибератак и кампаний по дезинформации, чтобы сдержать поддержку Украины в войне.

Прокремлевский хакерский коллектив под названием Killnet этим летом начал серию атак на западные правительственные сети и критическую инфраструктуру, громко заявив о победах в социальных сетях и российских СМИ и причинив головную боль органам безопасности противников России.

Killnet радикально отличается от российских высококвалифицированных хакеров, работающих на группы ее спецслужб, такие как Fancy Bear и Sandworm, которые получили известность благодаря взломам Национального комитета Демократической партии США и запуску разрушительной программы-вымогателя под названием NotPetya соответственно. Killnet, с другой стороны, больше похож на разъяренную националистическую онлайн-мафию, вооруженную низкокачественными кибернаступательными инструментами и тактикой. Его большой успех заключается в создании повествования о войне.

«Многие в России считают их героями, — сказал Стефан Соесанто, исследователь из Центра исследований безопасности ETH Zurich, отслеживающий деятельность хактивистов в конфликте. — Цель Killnet — заставить европейцев заплатить за их безоговорочную поддержку Украины и наказать Запад. правительств за их антироссийские настроения».

Группа прославилась запуском распределенных атак типа «отказ в обслуживании» (DDoS) и «порчей» веб-сайтов, на которых они размещают пророссийские сообщения на взломанных ими веб-сайтах. Впервые она появилась в январе как поставщик киберпреступников по найму, но когда российские танки вторглись в Украину в конце февраля, группировка быстро стала громко поддерживать наступление России.

«KillNet работает на эмоциях. Они ищут мести и возмездия за злодеяния, которые, по их мнению, были нанесены России и ее народу», — сказал исследователь, известный под своим онлайн-псевдонимом CyberKnow, который отслеживает группы угроз и публикует исследования на трекере кибербезопасности. CyberKnow попросил не раскрывать его настоящее имя. «Они крайне реакционно настроены по отношению к текущим геополитическим событиям».

В последние месяцы он был нацелен на более чем 10 западных стран, включая Латвию, Литву, Норвегию, Италию, США и совсем недавно Эстонию. Одно из самых громких нападений группы произошло в мае против песенного конкурса Евровидение. России запретили участвовать в конкурсе, поэтому хакерская группа предприняла попытку DDoS-атаки. Полицейское управление Италии предотвратило нападение, но не без ответных ударов страны по сайтам Сената и Национального института здравоохранения.

В июне нацеливание KillNet на Литву вывело ее на новый уровень популярности в российских СМИ, после того как Вильнюс ввел блокаду товаров на российскую территорию в Калининграде. В распространенном в сети видеообращении группа потребовала от Литвы разрешить транзит товаров в Калининград; в противном случае атаки будут продолжаться. В конечном итоге атака имела «ограниченный успех», по словам вице-министра национальной обороны страны Маргириса Абукявичюса, было удалено несколько веб-страниц, но внимание, которое она привлекла, было огромным.

Эстония стала мишенью 17 августа, но власти заявили, что атака на услуги электронного правительства прошла «практически незамеченной» гражданами Эстонии.

Специалисты по кибербезопасности описывают группу как скорее неприятность, чем угрозу. Большинство стран, подвергшихся его атакам, смогли отразить атаки или легко оправиться от них. В исследовательском документе, опубликованном в прошлом месяце, говорится, что роль хактивистских сообществ в войне на Украине была «незначительной». не может найти доказательств громких действий».

Но успех Killnet заключается не в его изощренности или способности взламывать, проникать и разрушать сети. Группа оставила свой след, громко заявив о своей победе, когда ей удалось заблокировать услуги — с хитрым пиаром, который включает в себя броские видеообъявления, мемы и изображения водяных знаков, которыми делятся в социальных сетях и сообщают новостные агентства.

Война столкнула Killnet с аналогичными коллективами, поддерживающими Киев. Хакерская группа Anonymous объявила войну России в начале конфликта, а украинское правительство мобилизовало свой внутренний ИТ-сектор и

сочувствующих ему людей из других стран для формирования «ИТ-армии Украины», которая координирует киберкампании и атаки на российские цели.

По словам исследователей, российские патриоты ведут тяжелую борьбу с широко поддерживаемыми украинскими хактивистами. «В отличие от Killnet, ИТ-армия невероятно настойчива в нацеливании на одну конкретную цель в течение недель или месяцев подряд, как список финансовых учреждений, которые они опубликовали в качестве целей в начале войны, — сказал Соесанто. — Они, вероятно, более эффективны, чем Killnet в 100 раз».

Killnet заявила, что хочет сотрудничать с российским правительством, но пока нет никаких признаков того, что она находится под непосредственным контролем чиновников.

Тем не менее, его четкая прокремлевская позиция может стать проблемой для России. «Это возлагает на Россию потенциальную ответственность за ущерб, причиненный такими операциями, если власти в Москве не дистанцируются от таких злонамеренных операций», — сказал Патрик Павляк, исполнительный директор Института исследований безопасности ЕС». ***(Antoaneta Roussi. Meet Killnet, Russia's hacking patriots plaguing Europe // POLITICO (https://www.politico.eu/article/meet-killnet-russias-hacking-patriots-plaguing-europe/). 09.09.2022).***

***

«В связи с усилением международной напряженности по мере того, как мы вступаем в восьмой месяц войны между Россией и Украиной, становится ясно, что наступает новая эра усиления атак, спонсируемых государством, особенно тех, которые нацелены на учреждения и службы государственного сектора.

Ранее в этом году Агентство по кибербезопасности и безопасности инфраструктуры (CISA) выпустило редкое предупреждение «Sheilds Up», подчеркнув необходимость того, чтобы американские организации сохраняли бдительность и защищали свои наиболее важные и конфиденциальные активы. Позже CISA также предупредила об угрозе, которую представляют спонсируемые государством злоумышленники из Китая и Северной Кореи.

Нынешний геополитический климат выдвинул кибербезопасность в центр внимания для обеспечения национальной безопасности, поэтому организациям государственного сектора особенно важно занимать активную позицию в отношении угроз. Упреждающая кибербезопасность начинается с полного понимания того, что необходимо защитить, и постоянной аналитики, необходимой для предотвращения вероятных атак.

Исследования показывают, что государственный сектор медленнее всего выявляет ключевые риски

Недавнее глобальное сравнительное исследование кибербезопасности показало, что среди всех опрошенных отраслей государственный сектор занимает первое место по неадекватному выявлению ключевых рисков. Это связано с тем, что государственный сектор продолжает бороться с разрозненными инфраструктурами, разрозненными операциями, децентрализованными практиками, ограниченностью ресурсов и несоответствием знаний, поскольку сегодняшняя картина угроз

усложнилась и ускорилась. В совокупности эти факторы вынуждают специалистов по безопасности оставаться в стороне и занимать оборонительную позицию при возникновении инцидентов, связанных с безопасностью, что позволяет как государственным субъектам угроз, так и рядовым операторам в равной степени осуществлять серьезные нарушения безопасности.

Более того, исследовательская лаборатория Skybox недавно обнаружила (PDF), что 186 уязвимостей, опубликованных в 2021 году, были оперативно проэксплуатированы в течение года, что на 24% больше, чем количество уязвимостей, опубликованных и впоследствии использованных в 2020 году. Это сокращает время между первоначальным обнаружением и активными эксплойтами и дает понять, что стратегия безопасности в организациях государственного сектора должна измениться.

Учитывая эти уникальные проблемы, с которыми сталкивается государственный сектор, злоумышленники все чаще проводят громкие атаки на эти организации. Векторы атак продолжают расширяться благодаря обнаружению новых уязвимостей в различных программах и приложениях. Эти уязвимости позволяют киберпреступникам проводить изощренные атаки с использованием скромных ресурсов.

Переход от реагирования к профилактике

Хорошей новостью является то, что организации могут следовать четким передовым методам для достижения упреждающего подхода к предотвращению кибератак.

Сосредоточьтесь на риске воздействия: визуализация всей поверхности атаки и понимание всех уязвимых точек имеет решающее значение для эффективной программы кибербезопасности. Однако продолжающийся поток вновь обнаруженных уязвимостей создает проблемы с расстановкой приоритетов и перегружает группы безопасности, которые часто имеют ограниченные ресурсы. Вместо того, чтобы тратить ограниченную полосу пропускания на поиск огромного количества уязвимостей, организации должны сосредоточиться на том, какие уязвимости подвержены угрозам и могут создать реальную угрозу сетевым активам.

Инвестируйте в автоматизацию: по-прежнему сложно найти специалистов по кибербезопасности, необходимых для эффективного противодействия современным угрозам. Поскольку ландшафт продолжает развиваться, организациям будет важно включить автоматизацию в свой стек инструментов, чтобы группы безопасности опережали злоумышленников. Эта технология уменьшит необходимость вручную отслеживать каждую уязвимость, поскольку данные продолжают экспоненциально расти.

Помните о всей цепочке поставок: организации должны пересмотреть свои бизнес-модели, чтобы убедиться, что их цепочки поставок влияют на их стратегии кибербезопасности, включая потенциальные уязвимости. Эта жизненно важная часть операции является колоссальной точкой возможной слабости. Некоторые из наиболее заметных нарушений за последние два года, в том числе SolarWinds и Kaseya, были прямым результатом уязвимостей, появившихся в цепочках поставок. По мере того, как эти цепочки становятся все более сложными и глобальными, а

доступ к ним выходит далеко за пределы организации, командам по безопасности будет крайне важно тщательно изучить потенциальные воздействия и уязвимости.

Достижение целостного подхода к кибербезопасности в государственном секторе

Контекст и информация необходимы для укрепления программ кибербезопасности государственного сектора. Повышая эффективность безопасности за счет создания стратегии управления состоянием безопасности, организации государственного сектора могут лучше визуализировать и анализировать гибридные, многооблачные и OT-сети, чтобы получить полную картину поверхности своих атак.

Это позволяет организациям опередить следующий инцидент безопасности, просматривая уязвимости так же, как это делают киберпреступники, сосредотачиваясь на уязвимостях с наивысшей оценкой риска и зная, могут ли они быть использованы и раскрыты или нет». ***(Ed Mosquera. How to improve public sector's security strategy? // Help Net Security (https://www.helpnetsecurity.com/2022/09/16/public-sector-security/). 16.09.2022).***

***

«Хакери масово атакують росіян, використовуючи їхній страх перед частковою мобілізацією, оголошеною президентом Росії Володимиром Путіним…

Як зафіксували експерти з кібербезпеки, після оголошення про мобілізацію в інтернеті з'явилася величезна кількість фішингових сайтів та розсилок від шахраїв, які пропонують отримати відстрочку, підроблені медичні довідки, термінову допомогу з переїздом тощо. Цьому сприяла велика кількість запитів у Google із фразами «відстрочка» та «хто в запасі».

Директор компанії «Антифішинг» Сергій Волдохін розповів ЗМІ, що вже відомі перші випадки шахрайства із використанням теми мобілізації. Злякавшись перспективи вирушити на війну, жертви купують у злочинців різні послуги, такі як «виключення зі списків мобілізованих». Найчастіше вони трапляються на фішингові сайти, але шахраї також дзвонять росіянам або їхнім близьким, обіцяючи «допомогу». Крім того, в інтернеті розміщують програми для перегляду списків мобілізованих або виїзду з РФ, які виявляються вірусними.

Організаціям надсилають листи з вимогами повідомити дані співробітників, щоб потім просто вкрасти. У випадку з компаніями такого сплеску поки не спостерігається, але деякі інциденти вже сталися.

Експерти зазначають, що будь-яка масштабна подія може спричинити хвилю інтернет-шахрайства. На тлі соціально значущих подій та суперечливої інформації увага людей стає розсіяною, а рішення частіше приймаються, керуючись емоціями, а не логікою. В результаті жертвами злочинців можуть стати навіть ті росіяни, які не схильні до традиційних способів шахрайства…» ***(Мобілізація в Росії: як хакери карають наляканих росіян в інтернеті // Фокус (https://focus.ua/uk/digital/530253-mobilizaciya-v-rossii-kak-hakery-nakazyvayut-ispugannyh-rossiyan-v-internete). 22.09.2022).***

***

«Исследователи безопасности обнаружили новую кампанию, нацеленную на несколько военных подрядчиков, занимающихся производством оружия, включая поставщика компонентов для истребителей F-35 Lightning II.

Целенаправленные атаки начинаются с рассылки фишинговых электронных писем сотрудникам, что приводит к многоступенчатому заражению с участием многих систем сохранения и предотвращения обнаружения.

Кампания выделяется своей безопасной инфраструктурой C2 и несколькими уровнями обфускации в стейджерах PowerShell.

Аналитики Securonixdiscovered обнаружили атаки, но не смогли связать кампанию с какими-либо известными субъектами угроз, хотя в отчете упоминается некоторое сходство с прошлыми атаками APT37 (Konni).

Ориентация на сотрудников

Фишинговое электронное письмо, нацеленное на сотрудников, включает в себя ZIP-вложение, содержащее файл-ярлык («Company & Benefits.pdf.lnk»), который при выполнении подключается к C2 и запускает цепочку сценариев PowerShell, заражающих систему вредоносным ПО.

Интересно, что файл ярлыка не использует широко используемые инструменты «cmd.exe» или «powershell.exe», а вместо этого полагается на необычную команду «C:\Windows\System32\ForFiles.exe» для выполнения команд.

Следующий шаг — распутать семиступенчатую цепочку выполнения PowerShell, характеризующуюся сложной обфускацией с использованием нескольких методов.

Методы запутывания, с которыми сталкиваются аналитики Securonix, включают запутывание переупорядочивания/символов, запутывание IEX, запутывание значений байтов, необработанное сжатие, изменение порядка, замену строк и запутывание обратных кавычек.

Кроме того, сценарий сканирует список процессов, связанных с программным обеспечением для отладки и мониторинга, проверяет, чтобы высота экрана превышала 777 пикселей, а объем памяти превышал 4 ГБ, чтобы избежать песочниц, а также убеждался, что система была установлена более трех дней назад.

Если какая-либо из этих проверок не пройдена, сценарий отключит системные сетевые адаптеры, настроит брандмауэр Windows на блокировку всего трафика, удалит все на всех обнаруженных дисках, а затем выключит компьютер.

Единственный случай, когда вредоносное ПО выходит, не причинив никакого вреда, — это когда язык системы установлен либо на русский, либо на китайский.

Если все проверки пройдены успешно, сценарий отключает ведение журнала блоков сценариев PowerShell и добавляет исключения Защитника Windows для файлов «.lnk», «.rar» и «.exe», а также для каталогов, важных для функционирования вредоносного ПО.

Постоянство достигается с помощью нескольких методов, включая добавление новых ключей реестра, встраивание сценария в запланированное задание, добавление новой записи в каталог автозагрузки, а также подписки WMI.

После того, как этап PowerShell завершает процесс, с C2 загружается окончательная полезная нагрузка ("header.png"), зашифрованная с помощью AES.

«Хотя мы смогли загрузить и проанализировать файл header.png, мы не смогли его расшифровать, поскольку считаем, что кампания завершена, и наша теория заключается в том, что файл был заменен, чтобы предотвратить дальнейший анализ», — объясняют исследователи.

«Наши попытки декодировать полезную нагрузку приведут только к мусорным данным».

C2 инфраструктура

Аналитики определили, что домены, используемые для инфраструктуры C2, поддерживающей эту кампанию, были зарегистрированы в июле 2022 года и размещены на DigitalOcean.

Позже злоумышленники переместили домены в Cloudflare, чтобы воспользоваться ее CDN и службами безопасности, включая маскировку IP-адресов, геоблокировку и шифрование HTTPS/TLS.

Некоторые домены C2, упомянутые в отчете, включают «terma[.]wiki», «terma[.]ink», «terma[.]dev», «terma[.]app» и «cobham-satcom.onrender[.] ком".

В целом, эта кампания выглядит как работа изощренного злоумышленника, который знает, как скрыться от радаров, поэтому обязательно проверьте поисковые запросы и общие IoC в отчете Securonix». ***(Bill Toulas. Stealthy hackers target military and weapons contractors in recent attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/stealthy-hackers-target-military-and-weapons-contractors-in-recent-attack/). 28.09.2022).***

***

«Mandiant, дочірня компанія Google, виявила докази того, що російська військова розвідка ГРУ координує свої дії з трьома проросійськими хактивістськими групами.

Нагадаємо, Mandiant стала частиною Google в результаті придбання за 5,4 мільярда доларів, яке завершилося на початку цього місяця. Вона надає послуги з кібербезпеки, які допомагають компаніям реагувати на витоки даних в їх корпоративних мережах. Крім того, Mandiant збирає дані про хакерську активність.

Як повідомляє The Wall Street Journal, протягом останніх кількох місяців Mandiant спостерігала за тим, що схоже на координацію між російською військовою розвідкою ГРУ і трьома хактивістськими групами - XakNet Team, Infocentr і CyberArmyofRussia_Reborn.

Кібератаки, виявлені Mandiant за останні місяці, включали чотири проломи, в яких ГРУ розмістило в мережах організацій шкідливе програмне забезпечення для знищення даних. Протягом 24 годин після кожного зломів хактивісти публікували дані, викрадені у компаній, на які було спрямоване шкідливе програмне забезпечення для знищення даних.

Одна з хактивістських груп, названих у звіті, Killnet, здійснила DDoS-атаки на організації в Японії, Італії, Норвегії, Естонії та Литві.

Веб-сайти урядових установ Литви зазнали щонайменше двох хвиль DDoS-атак у червні цього року, повідомляє сьогодні журнал. Відповідальність за деякі з атак взяла на себе організація Killnet. Повідомляється, що DDoS-кампанії були

незвичайними, оскільки вони були «нецілеспрямованими і ніколи не досягали руйнівного рівня», але продовжувалися протягом значного проміжку часу.

Killnet також взяла на себе відповідальність за хвилю DDoS-атак, спрямованих на організації в Естонії в серпні цього року. Хакери відправляли до 200 гігабайт даних в секунду на системи організацій, намагаючись вивести їх з ладу, йдеться в звіті. Естонія успішно відбила ці DDoS-атаки.

The Wall Street Journal повідомляє також, що було «кілька інцидентів», спрямованих на організації в США. Congress.gov, офіційний веб-сайт для законодавчої інформації Конгресу, в червні в результаті DDoS-атаки було заблоковано приблизно на дві години. У серпні Killnet заявив про початок кібератаки на Lockheed Martin і опублікував документи, які, за його словами, були викрадені у компанії Gorilla Circuits, постачальника оборонної промисловості, що займається виробництвом друкованих плат.

«Ми ніколи раніше не спостерігали такого обсягу кібератак, різноманітності суб'єктів загрози і координації зусиль протягом декількох місяців», - заявили дослідники Mandiant». ***(Google знайшла докази координаційної роботи росії з хакерами // Компьютерное Обозрение (https://ko.com.ua/google_znajshla_dokazi_koordinacijnoyi_roboti_rosiyi_z_hakerami_142176). 26.09.2022).***

***

Створення та функціонування кібервійськ

«Командование космических операций США назначает специалистов по кибербезопасности и разведке для работы бок о бок с операторами спутников, чтобы они были лучше подготовлены к защите систем США от электронных и физических угроз, сказал генерал-майор Дуглас Шисс.

«Мы готовимся и готовимся к бою», — сказал Шисс 19 сентября на конференции Air, Space & Cyber.

Шисс является заместителем командующего Командованием космических операций Космических сил, а также курирует компонент объединенных сил Космического командования США на базе космических сил Ванденберг в Калифорнии.

Командование космических операций, базирующееся в Петерсон-Спейс-Бэй, штат Колорадо, имеет несколько эскадрилий киберспециалистов, которые поддерживают военные подразделения, эксплуатирующие спутники связи, наблюдения и навигации. По словам Шисса, в следующем году будет добавлено больше, чтобы обеспечить адекватную киберзащиту всех спутниковых устройств.

Космические силы следуют директиве министра ВВС Фрэнка Кендалла о защите космических систем от кибератак, которые такие соперники, как Китай, попытаются предпринять во время конфликта.

«С первых дней работы я говорил, что моими приоритетами были Китай, Китай и еще раз Китай… и мне хотелось бы думать, что это сообщение начинает

находить отклик», — сказал Кендалл в понедельник в своем программном выступлении на конференции.

Шисс сказал, что одним из самых последних действий было назначение киберотряда исключительно для работы с операторами спутников космической инфракрасной системы (SBIRS), которые обеспечивают раннее предупреждение о запусках ракет.

«Они находятся прямо там, в одном здании с нашими операторами предупреждения о космосе и ракетах», — сказал Шисс. «Мы собираемся продолжать это делать».

В ответ на обеспокоенность Пентагона по поводу китайского и российского противоспутникового оружия, Космические силы также добавляют разведывательные подразделения к подразделениям спутниковых операций, чтобы операторы получали точную информацию о возможных угрозах.

«Это сокращает время, необходимое операторам для получения информации, с дней до минут», — сказал Шисс.

«Очевидно, как вы слышали сегодня от госсекретаря и других, наши близкие конкуренты продолжают модернизировать свои силы», — добавил он. «Мы должны продолжать осуществлять операции, управляемые интеллектом, чтобы мы могли быстрее принимать решения и иметь возможность опередить своих ближайших конкурентов».

Шисс сказал, что приоритетом в будущем является модернизация инфраструктуры обучения и тестирования Космических сил, чтобы стражи могли отрабатывать миссии в боевой обстановке, а живучесть спутников можно было более точно проверять.

Космические силы создали в Петерсоне отдельное Командование космической подготовки и готовности, чтобы сосредоточиться на обучении и испытаниях. «Они планируют создать национальный центр космической подготовки и испытаний», — сказал Шисс. «И мы в Командовании космических операций, вероятно, самые большие сторонники того, чтобы помочь им сделать это». ***(Sandra Erwin. Space Force shifting resources to intelligence and cybersecurity // SpaceNews (https://spacenews.com/space-force-shifting-resources-to-intelligence-and-cybersecurity/). 19.09.2022).***

***

Кіберзахист критичної інфраструктури

«Агентство кибербезопасности и безопасности инфраструктуры проведет следующие три года, оценивая успех усилий правительства по защите критической инфраструктуры, контролируемой государством и частными лицами, от кибератак.

Согласно только что обнародованному агентством национальному плану на период до 2025 года, стратегия CISA будет включать цели по производительности, которые должны были быть поставлены в конце июля в соответствии с меморандумом о национальной безопасности, касающимся кибербезопасности для

промышленных систем управления, используемых в критической инфраструктуре. Агентство планирует выпустить их где-то в октябре — месяце осведомленности о кибербезопасности, — заявил в четверг исполнительный помощник директора CISA по кибербезопасности Эрик Гольдштейн перед законодателями из Комитета внутренней безопасности Палаты представителей.

«При необходимости в рамках органов CISA мы будем устанавливать стандарты и рекомендации для принятия решений в области безопасности, так же как и наши усилия по установлению целей производительности и повышению межотраслевого базового уровня кибербезопасности», — говорится в плане CISA.

Измерение прогресса в области кибербезопасности было общеизвестным больным вопросом с самого начала целенаправленных усилий по выработке политики по этому вопросу. Возвращаясь к 2013 году, когда Национальный институт стандартов и технологий начал работу над своей знаковой структурой кибербезопасности для критически важной инфраструктуры, возникла необходимость оценивать состояние кибербезопасности на основе результатов, а не степени, в которой организации внедряли определенные средства контроля.

Промышленность постоянно полагалась на соответствующие аргументы, пытаясь помешать усилиям — совсем недавно член палаты представителей Джим Ланжевен, доктор медицинских наук, приложил поправку к Закону о полномочиях национальной обороны в Палате представителей — чтобы привлечь их к ответственности за определенные стандарты кибербезопасности.

«В течение нескольких лет федеральные, государственные и местные органы власти и промышленность использовали модель партнерства для защиты критически важной инфраструктуры, большая часть которой принадлежит частному сектору и управляется ею, от национальных и криминальных кибератак. Этот подход оказался в значительной степени успешным», — говорится в письме, направленном Торговой палатой США и другими представителями крупных компаний лидерам комитетов Сената в пятницу против поправки. «Многие сосредотачиваются на происходящих досадных киберинцидентах, но слишком немногие сосредотачиваются на бесчисленных кибератаках, которых удалось избежать».

Директор CISA Джен Истерли, например, больше не желает принимать такие заявления об успехе как данность. Во время недавнего заседания ее Консультативного совета по кибербезопасности она отметила важность проекта, который агентство собирается приступить.

«Мы действительно будем усердно работать, чтобы согласовать наши цели и задачи с конкретными показателями, которые помогут нам снизить риск», — сказал Истерли, ссылаясь на план. «Это не тривиальная попытка. Как мы знаем, легко подсчитать показатели производительности. Гораздо сложнее измерить эффективность и результаты. Но мы считаем, что это невероятно важно, учитывая нашу миссию, которая заключается в том, чтобы возглавить национальные усилия по пониманию, управлению и снижению рисков для критически важной инфраструктуры, на которую американцы полагаются каждый час каждого дня».

Успех плана CISA зависит от многих внешних факторов. Среди них будет его способность собирать необходимые данные, в том числе посредством реализации

Закона об отчетах о кибер-инцидентах для критически важной инфраструктуры, который вступил в силу в марте.

Некоторые представители сообщества кибербезопасности, в том числе сенатор Марк Уорнер, штат Вирджиния, отметили отсутствие надлежащего правоприменительного механизма, побуждающего компании сообщать о нарушениях безопасности и соответствующей информации в CISA. В сентябре 2021 года Истерли вместе с Национальным директором по кибербезопасности Крисом Инглисом и федеральным директором по информационной безопасности Крисом Де Рушей выступили за включение финансовых санкций за несоблюдение в новый закон, который, по словам Уорнер, стал «беззубым» после того, как такие меры были отменены. оригинальное предложение, которое он написал.

С тех пор Истерли более полно воспринял роль CISA как места, где промышленность может искать утешения в контроле за соблюдением нормативных требований и вместо этого привлекать промышленность к участию в плане агентства с помощью пряников, таких как доступ к правительственной разведке и ресурсам для поиска уязвимостей и реагирования на инциденты. Такие обмены являются целью таких механизмов, как Объединенное сотрудничество по киберзащите CISA и других организационных структур, где агентство регулярно получает информацию от крупных компаний из различных отраслей.

Но в то время как в прошлом июльском меморандуме по национальной безопасности, призывающем к установлению целей CISA, говорится, что инициатива направлена на добровольное сотрудничество отрасли с правительством, поправка Ланжевена — наряду с комментариями официальных лиц Белого дома — предлагает попытку связать предстоящие цели производительности с потенциальными регуляторными усилиями.

Выступая этим летом на мероприятии Центра новой американской безопасности, советник по национальной безопасности по кибербезопасности и новым технологиям Энн Нойбергер заявила, что Белый дом работает с законодателями, чтобы стимулировать агентства использовать свои регулирующие полномочия для управления рисками кибербезопасности в своих секторах.

Поправка Ланжевена отражает меморандум национальной безопасности по промышленным системам управления. Они оба говорят, что Министерству внутренней безопасности следует работать с соответствующими агентствами для разработки межотраслевых и отраслевых целей эффективности кибербезопасности.

«Эти цели производительности должны служить четким руководством для владельцев и операторов в отношении методов и подходов к кибербезопасности, которым американцы могут доверять и должны ожидать таких важных услуг», — говорится в обоих документах, добавляя: «Эти усилия могут также включать изучение того, дополнительные юридические полномочия были бы полезны для повышения кибербезопасности критической инфраструктуры, которая жизненно важна для американского народа и безопасности нашей страны».

Во время слушаний в Комитете по внутренней безопасности Палаты представителей в четверг член палаты представителей Иветт Кларк, DN.Y., которая возглавляет подкомитет по кибербезопасности и инновациям, спросила

Гольдштейна о том, в какой степени CISA запрашивала информацию о целях производительности от ряда заинтересованных сторон.

«Мы прошли два раунда надежных отзывов заинтересованных сторон, оба из которых включали публичную проверку», — сказал Гольдштейн. «Примечательно, что мы получили более 2000 комментариев по целям эффективности кибербезопасности и провели различные семинары, в том числе как для отраслевых партнеров, так и для широкой общественности, а также слушания для наших групп заинтересованных сторон».

Он добавил, что агентство хотело расширить сферу своей деятельности за пределы заинтересованных сторон, с которыми они общаются каждый день в рамках CISA.

«Итак, мы обратились исключительно к нашим международным партнерам, академическим кругам, исследователям, владельцам-операторам, производителям устройств, интеграторам и другим организациям», — сказал Гольдштейн.

Но только несколько комментариев — от представителей индустрии информационных и коммуникационных технологий, которые критиковали предварительные цели производительности — были опубликованы, а другие представители отрасли заявили, что CISA с пониманием отнеслась к их отзывам. Представитель CISA сообщил Nextgov, что агентство не намерено публиковать полученные комментарии. CISA не объяснила причину своего решения, а также отклонила просьбу предоставить более ранние версии целей производительности, на которые есть ссылки на их веб-сайте.

Взаимодействие с промышленностью по целям производительности осуществляется через Консультативный совет партнерства по критически важной инфраструктуре, созданный в 2006 г. и постоянно обновляемый, последний раз в ноябре 2020 г., и освобожден от законов об общественной прозрачности в соответствии с Законом о внутренней безопасности. Но заседание консультативного комитета во вторник дало представление о том, как крупнейшие компании в экономике могут надеяться повлиять на их заявки отраслевыми агентствами по управлению рисками.

Поправка Ланжевена требует, чтобы межведомственный совет под председательством директоров CISA и Управления национального кибер-директора определил список не более чем из 200 системно важных субъектов, для которых будут актуальны цели деятельности, и назначил агентства для их регулирования, где необходимый. Во время встречи во вторник председатель Том Фаннинг, генеральный директор электроэнергетической компании Southern Company, рекомендовал частному сектору участвовать в выявлении таких организаций и принятии решений агентствами по управлению отраслевыми рисками.

«Мы также хотим привлечь системно значимые субъекты к выявлению первой, второй и третьей производной того, что создает и проявляет себя как риск», — сказал он. И хотя меморандум Белого дома и поправка Ланжевена просят соответствующие ведомства активно изучить необходимость дополнительных полномочий и регулирующих мер, Фаннинг обязался оставаться как можно ближе к статус-кво.

«Мы хотим наметить обязательства системообразующих [организаций] по достижению национальных целей устойчивости», — сказал он о рекомендациях,

которые комитет позже одобрил в полном составе. «Мы обязуемся… оптимизировать и сделать «умными» — на основе хороших результатов — существующее регулирование и, возможно, упростить его… гармонизировать регулирование и, по возможности, опираться на то, что уже существует». ***(Mariam Baksh. But big companies want to avoid agencies' use of related performance goals in new regulation // Nextgov (https://www.nextgov.com/cybersecurity/2022/09/cisa-plans-measure-effect-coming-standards-industrys-cybersecurity/377363/). 19.09.2022).***

***

«Стандартные подходы к безопасности операционных технологий (OT) и промышленных систем управления (ICS) «неадекватно справляются с текущими угрозами», заявили Агентство по кибербезопасности и безопасности инфраструктуры (CISA) и Агентство национальной безопасности (АНБ) в совместном бюллетене по кибербезопасности, направленном на объектах критической инфраструктуры.

«Устройства и конструкции OT/ICS общедоступны, часто содержат уязвимые компоненты информационных технологий (ИТ), а также включают внешние соединения и удаленный доступ, которые увеличивают возможности для атак», — говорится в бюллетене.

«Кроме того, существует множество инструментов для использования ИТ- и OT-систем. В результате этих факторов злоумышленники в киберпространстве представляют растущий риск для сетей АСУ».

Основываясь на предыдущем руководстве CISA и NSA, CISA выпустила рекомендацию, чтобы пролить свет на тактику, методы и процедуры (TTP), используемые злоумышленниками, чтобы помочь владельцам и операторам OT и ICS лучше защитить свои активы.

Использование технологий, которым уже несколько десятков лет, и растущая популярность конвергенции OT и ИТ расширили поверхность атаки, когда речь идет о безопасности OT и АСУ ТП, говорится в консультативном заключении.

Организации в секторе здравоохранения и в других местах все чаще используют киберфизические системы, которые включают элементы ИТ в устройства и инфраструктуру OT. Хотя такая интеграция может повысить эффективность и действенность, она также может подвергнуть организации дополнительным рискам безопасности.

Владельцы и операторы ICS и OT должны принимать взвешенные и взвешенные решения по обеспечению безопасности, чтобы ограничить раскрытие конфиденциальных данных. В то время как традиционные кибератаки на основе ИТ представляют собой более обычную угрозу, CISA и АНБ подчеркнули важность поддержания осведомленности о кибербезопасности и обеспечения безопасности активов OT и ICS.

КАК ВЫГЛЯДИТ КИБЕРАТАКА ICS/OT?

«Сегодня киберсфера заполнена хорошо финансируемыми злоумышленниками, финансируемыми национальными государствами, а также менее изощренными группами, независимыми хакерами и внутренними угрозами», — говорится в бюллетене.

«В последние годы различные злоумышленники стали мишенью систем управления для достижения политических целей, экономических преимуществ и, возможно, разрушительных последствий. Совсем недавно участники APT также разработали инструменты для сканирования, компрометации и управления целевыми OT-устройствами».

CISA и АНБ отметили, что субъекты угроз обычно выполняют следующие шаги для выполнения атак на критически важные системы управления инфраструктурой:

Установите предполагаемый эффект и выберите цель.

Соберите информацию о целевой системе.

Разработайте методы и инструменты для навигации и управления системой.

Получите первоначальный доступ к системе.

Используйте приемы и инструменты для достижения желаемого эффекта.

«Используя определенный опыт и знания сети, злоумышленники, такие как представители национального государства, могут предпринимать эти шаги скоординированным образом, иногда одновременно и неоднократно, как показано в реальной кибератиности», — говорится в бюллетене. инфраструктура и многочисленные попытки вторжения спонсируемых государством российских кибератак в энергетический сектор США.

В бюллетене также представлены подробные пояснения по каждому из 5 шагов.

ТАКТИКА СМЯГЧЕНИЯ ПОСЛЕДСТВИЙ

«Сложность баланса сетевой безопасности с производительностью, функциями, простотой использования и доступностью может оказаться непосильной для владельцев/операторов. Это особенно верно, когда системные инструменты и сценарии упрощают использование и повышают доступность или функциональность сети управления; а также когда поставщикам оборудования требуется удаленный доступ для соблюдения гарантийных обязательств, выполнения обязательств по обслуживанию и финансовых/биллинговых функций», — поясняется в бюллетене.

«Однако с ростом числа нацеливаний OT/ICS со стороны злоумышленников владельцы/операторы должны лучше осознавать риски при принятии этих балансирующих решений. Владельцы/операторы также должны тщательно продумать, какая информация об их системах должна быть общедоступной, и определить, действительно ли необходимо каждое внешнее подключение».

В бюллетене также отмечается, что распространение доступных решений для обеспечения безопасности может оказаться непосильным для операторов АСУ ТП и OT, что «приводит к параличу выбора».

CISA и АНБ рекомендовали организациям использовать несколько простых стратегий для смягчения реальных угроз. Например, организациям следует сосредоточиться на ограничении доступа к системной информации и по возможности избегать раскрытия информации об аппаратном, микропрограммном или программном обеспечении системы.

«Распространяйте только те данные, которые необходимы для соблюдения применимых правовых требований, таких как те, которые требуются поставщиками по контракту, — не более того», — подчеркивается в бюллетене.

Кроме того, владельцы и операторы должны определять и защищать удаленные точки доступа, ограничивать доступ к системе управления и сетевым приложениям, инструментам и сценариям, а также проводить регулярные аудиты безопасности. Наконец, в бюллетене рекомендуется, чтобы организации внедрили динамическую сетевую среду, периодически внося управляемые изменения в сеть, такие как изменение пулов IP-адресов или обновление операционных систем.

Однако агентства признали, что «во многих средах OT/ICS может быть нереально вносить регулярные некритические изменения». Тем не менее, небольшие периодические изменения могут иметь большое значение.

«Сочетание интегрированных, упрощенных инструментов и удаленного доступа создает среду, которая позволяет злоумышленникам атаковать сети систем управления. Новые средства доступа с поддержкой ИТ открывают киберсубъектам более широкую поверхность для атак в киберфизических средах», — говорится в заключении бюллетеня.

«Защитникам OT/ICS жизненно важно предвидеть TTP кибер-актеров, сочетающих ИТ-опыт с инженерными ноу-хау. Защитники могут использовать меры, перечисленные в этом бюллетене, чтобы ограничить несанкционированный доступ, заблокировать инструменты и потоки данных и помешать злоумышленникам достичь желаемых результатов». ***(Jill McKeon. CISA, NSA Provide OT, ICS Defense Strategies to Critical Infrastructure // TechTarget, Inc. (https://healthitsecurity.com/news/cisa-nsa-provide-ot-ics-defense-strategies-to-critical-infrastructure). 27.09.2022).***

***

Захист персональних даних

«За повідомленням видання Bloomberg додаток TikTok був зламаний. У понеділок кілька аналітиків з кібербезпеки написали в Твіттері про виявлення імовірного злому небезпечного сервера, який дозволив отримати доступ до сховища TikTok, яке, на їхню думку, містило особисті дані користувачів, включаючи платіжні.

Усього за кілька днів до цього корпорація Microsoft заявила, що виявила серйозну вразливість у TikTok, яка дозволяє зламувати облікові записи в один клік. Представник TikTok розповів, що компанія швидко відреагувала на висновки Microsoft і усунула вразливість у системі безпеки, яка була помічена у деяких старих версіях додатка для Android. Також він зазначив, що заяви про злом, виявлений на вихідних, помилкові:

«Наша група безпеки вивчила цю заяву і визначила, що код, що розглядається, абсолютно не пов’язаний з вихідним кодом серверної частини TikTok»

Рой Хант, австралійський експерт з кібербезпеки, переглянув деякі зразки даних, перелічених у файлах, що просочилися, і поки не впевнений, що це дійсно злом — частина даних реальна, частина ні, якісь детальні дані і так публічно

доступні, тому чіткої думки, що це не компіляція, він не має. Інші експерти пишуть, що доступна вся база — а це понад мільярд користувачів.

Поки що витік офіційно ніхто не коментує — що ще й спричинено тим, що у США сьогодні вихідний, День Праці». ***(Bloomberg: Є вірогідність, що хакери зламали TikTok і отримали доступ до платіжних даних користувачів // PaySpace Magazine (https://psm7.com/uk/security/bloomberg-vozmozhno-xakery-vzlomali-tiktok-i-poluchili-dostup-k-platezhnym-dannym-polzovatelej.html). 05.09.2022).***

***

Менеджер паролей LastPass говорит, что злоумышленники, стоящие за августовским инцидентом безопасности, имели доступ к его системам в течение четырех дней.

Генеральный директор LastPass Карим Тубба, поделившись подробностями о взломе в прошлом месяце, подтверждает, что нет никаких свидетельств активности каких-либо злоумышленников за пределами установленного срока.

«Мы также можем подтвердить, что нет никаких доказательств того, что этот инцидент связан с каким-либо доступом к данным клиентов или зашифрованным хранилищам паролей», — говорит Тубба.

В августе неизвестный злоумышленник получил несанкционированный доступ к исходному коду и служебной технической информации LastPass...

Детали расследования

Расследование взлома было проведено в партнерстве с фирмой по кибербезопасности Mandiant и показало, что деятельность злоумышленника ограничивалась четырехдневным периодом, пока инцидент не был локализован.

Дальнейшее расследование, проведенное LastPass и Mandiant, показало, что злоумышленники получили доступ к среде разработки, используя скомпрометированную конечную точку разработчика.

«Хотя метод, использованный для первоначальной компрометации конечной точки, неубедителен, злоумышленник использовал свой постоянный доступ, чтобы выдать себя за разработчика после того, как разработчик успешно прошел аутентификацию с помощью многофакторной аутентификации», — говорит Тубба.

Тубба признает, что злоумышленник смог получить доступ к среде разработки, но не смог получить доступ ни к каким данным клиентов или зашифрованным хранилищам паролей.

Тубба также говорит, что среда разработки LastPass физически отделена от других сред, включая производственную зону, и не имеет данных клиентов или зашифрованных хранилищ.

В уведомлении также говорится, что у компании нет доступа к мастер-паролям, используемым клиентами, и без мастер-пароля никто не может расшифровать данные хранилища в рамках «модели безопасности с нулевым разглашением».

Компания подтверждает, что ее код остается неповрежденным, и нет никаких доказательств отравления кода или внедрения вредоносного кода.

«Разработчики не имеют возможности передавать исходный код из среды разработки в рабочую среду. Эта возможность ограничена отдельной командой по

сборке и выпуску и может быть реализована только после завершения тщательного анализа кода, тестирования и проверки», — говорит Тубба.

LastPass также сотрудничает с неназванной фирмой по кибербезопасности для дальнейшего совершенствования своих методов обеспечения безопасности исходного кода, включая безопасные процессы жизненного цикла разработки программного обеспечения, моделирование угроз, управление уязвимостями и программы вознаграждения за ошибки в рамках своей программы управления рисками.

Компания заявляет, что развернула дополнительные меры безопасности, в том числе дополнительные средства контроля безопасности и мониторинга конечных точек, а также развернула возможности анализа угроз, а также усовершенствованные технологии обнаружения и предотвращения для сред разработки и производства.

Это не первый раз, когда LastPass становится мишенью для хакеров, включая инцидент 2015 года, когда злоумышленники убегают с именами пользователей и хешированными мастер-паролями...

Эксперты по безопасности продолжают рекомендовать менеджеры паролей в качестве передовой практики. Исследование 2019 года показало, что надежность пароля значительно возрастает, когда пользователи используют приложение для управления паролями». **(Prajeet Nair. Hacker Accessed LastPass Internal System for 4 Days // Information Security Media Group, Corp. (https://www.govinfosecurity.com/hacker-accessed-lastpass-internal-system-for-4-days-a-20098). 17.09.2022).**

***

«Uber утверждает, что злоумышленник, стоящий за кибератакой на прошлой неделе, не имел доступа к производственной среде компании, учетным записям пользователей или базам данных, которые она использует для хранения конфиденциальной информации.

Компания по доставке еды и поездок в обновлении безопасности в понедельник заявила, что не нашла доказательств того, что ее кодовая база была изменена, а также не было доступа к каким-либо данным клиентов или пользователей, хранящимся у ее облачных провайдеров.

Злоумышленник, тем не менее, получил доступ и удалил сообщения Slack, данные для инструмента, который финансовая команда Uber использует для управления счетами, и панель управления компании в HackerOne, где хранятся отчеты об уязвимостях.

«Все отчеты об ошибках, к которым злоумышленник смог получить доступ, были исправлены», — говорится в сообщении компании.

Uber после первоначального расследования заявил, что злоумышленник взломал учетную запись подрядчика. Компания заявила, что злоумышленник, вероятно, приобрел корпоративный пароль человека в даркнете после того, как его личное устройство было заражено вредоносным ПО, что раскрыло его учетные данные.

Злоумышленник инициировал атаку усталости от многофакторной аутентификации, в ходе которой он неоднократно пытался войти в учетную запись Uber подрядчика, что вызывало запросы двухфакторной аутентификации.

По словам Uber, подрядчик в конечном итоге принял один из этих запросов, что позволило злоумышленнику успешно войти в систему.

Uber возложил вину за кибератаку на прошлой неделе на злоумышленника, связанного с Lapsus$, группой вымогателей, ответственной за атаки в этом году на Cisco, Nvidia, Microsoft, Okta, Samsung и, как сообщается, Rockstar Games в минувшие выходные.

Uber заявил, что тесно координирует усилия по восстановлению и реагированию с ФБР и Министерством юстиции. Компания также обязалась усилить свою киберполитику, методы и технологии для улучшения своей защиты.

Службы Uber не пострадали от атаки и продолжают работать. Компания пока не ответила на запросы о комментариях.

«Оттуда злоумышленник получил доступ к нескольким другим учетным записям сотрудников, что в конечном итоге дало злоумышленнику повышенные права доступа к ряду инструментов, включая Google Workspace и Slack», — говорится в сообщении компании.

Злоумышленник разместил сообщение на общекорпоративном канале Slack и перенастроил OpenDNS Uber для «отображения графического изображения сотрудникам на некоторых внутренних сайтах», говорится в сообщении компании.

Uber не объяснил, как злоумышленник получил доступ к учетным записям других сотрудников после того, как учетная запись подрядчика была скомпрометирована.

Компания заявила, что приняла несколько защитных мер в ответ на атаку:

Скомпрометированные или потенциально скомпрометированные учетные записи были идентифицированы и заблокированы или требовали сброса пароля для восстановления доступа.

Многие внутренние инструменты были отключены.

Параметры доступа были сброшены для многих внутренних сервисов Uber путем смены ключей.

Кодовая база компании была заблокирована, что предотвратило любые новые изменения кода.

Когда Uber восстановил доступ к внутренним инструментам, он потребовал от сотрудников повторной аутентификации учетных данных». ***(Matt Kapko. Uber details how it got hacked, claims limited damage // Industry Dive (https://www.cybersecuritydive.com/news/uber-attack-details/632193/). 19.09.2022).***

***

«Свидетельские показания в Конгрессе от Пейтера Затко — легендарного прародителя программ раскрытия уязвимостей для кибербезопасности — дали представление о том, как Twitter маневрировал в рамках правоприменительного процесса Федеральной торговой комиссии, уклоняясь от ответственности за управление данными пользователей, которыми, по его словам, прискорбно пренебрегали в пользу увеличения прибыли.

«Главный офицер по вопросам конфиденциальности прямо сказал мне, что FTC пришла и спросила: «Удаляет ли Twitter информацию о пользователях, когда они покидают платформу?», — сказал Затко. — И причина, по которой этот человек сказал мне это, [является] он сказал: «Мне нужно, чтобы вы это знали, потому что другие регулирующие органы спрашивают нас, и эта уловка не выдержит». Поэтому вместо того, чтобы ответить, удаляем ли мы пользовательские данные, мы намеренно ответили: «Мы деактивируем пользователей».

Во вторник Затко дал показания перед Юридическим комитетом Сената о раскрытии информации о деятельности Twitter Министерству юстиции, Комиссии по ценным бумагам и биржам и Федеральной торговой комиссии в июле, как раз в тот момент, когда Илон Маск пытался отказаться от запланированного приобретения компании.

Причина, по которой Twitter не может подтвердить FTC, что они удаляют пользовательские данные, заключается в том, что они знают только около 20% данных, которые они собирают от пользователей, сказал Затко. Он подробно описал среду без каких-либо элементов управления или базового ведения журналов для ответственного управления или защиты подавляющего большинства пользовательских данных и действий, к которым, по его словам, в результате получили доступ тысячи сотрудников — примерно половина компании. Это и другие плохие методы обеспечения безопасности ставят Twitter в нарушение нескольких законов и правил, а также постановления о согласии Федеральной торговой комиссии от 2011 года, сказал Затко в своем раскрытии.

Впервые привлек внимание к уязвимостям безопасности в таких компаниях, как Microsoft в 1990-х годах, Затко продолжил работу над разработкой инструментов кибербезопасности для Агентства перспективных исследовательских проектов Министерства обороны, а также работал в Google, прежде чем был нанят Twitter в ноябре 2020 года, когда компания пошатнулась от крупного скандала с безопасностью. Подростки могли публиковать сообщения со счетов Маска, бывшего президента Барака Обамы и других, заманивая жертв в мошенничество, связанное с биткойнами.

Ссылаясь на свой опыт работы в правительстве, Затко рассказал законодателям о последствиях для национальной безопасности, которые сосредоточились на сообщениях о том, что китайская разведывательная служба получает доступ к Твиттеру. По его словам, такие агенты не выполняли бы свою работу, если бы не были в Твиттере, который является золотой жилой для шпионов.

Во время слушаний Затко, более известный как «Мадж», сказал, что руководители Twitter гораздо больше боятся французского правительства, которое, по его словам, использует поддающиеся проверке и поддающиеся количественной оценке механизмы в своей правоприменительной деятельности, чем FTC, о чем он сказал. по сути, позволяет компаниям «самостоятельно оценивать свою домашнюю работу».

«Было много оценок и проверок, которые представляли собой вопросы для интервью», — сказал он о процессе FTC для обеспечения соблюдения приказа 2011 года, согласно которому Twitter должен улучшить свою безопасность после предыдущих компрометаций. «Ты сделал все лучше? Да, мы сделали, хорошо,

проверьте. Наземной правды было не так много. Количественных измерений было немного».

Затко сказал, что даже когда Федеральная торговая комиссия использует свои правоприменительные полномочия, ее разовые штрафы не так эффективны, как институциональные изменения и практика, на которые полагаются европейские коллеги. Он также поднял проблемы со сторонними сертификаторами безопасности. «Изрядное количество интервью было получено от компаний-аудиторов, которых Twitter смог нанять самостоятельно. Я думаю, что это немного похоже на конфликт интересов», — сказал он.

Законодатели по обе стороны прохода воспользовались возможностью поставить под сомнение способность FTC обеспечить соблюдение режима конфиденциальности и безопасности данных в соответствии с новым законодательством по этому вопросу. Они казались сбитыми с толку перспективой того, что Twitter будет намеренно пренебрегать такими серьезными проблемами национальной безопасности. Мадж заверил их, что можно ответственно защищать пользовательские данные и отслеживать попытки вторжения, но сказал, что компания и другие компании в технологической отрасли сосредоточены на других приоритетах, таких как увеличение доходов». ***(Mariam Baksh. Whistleblower Explains How Twitter Easily Skirted FTC's Data Security Enforcement // Nextgov (https://www.nextgov.com/cybersecurity/2022/09/whistleblower-explains-how-twitter-easily-skirted-ftcs-data-security-enforcement/377130/). 14.09.2022).***

***

«Компания The North Face, производящая одежду для активного отдыха, подверглась атаке с использованием учетных данных, в результате которой было скомпрометировано более 194 905 учетных записей. По данным Bleeping Computer, The North Face разослала письма с уведомлением об утечке данных и инициировала сброс паролей для затронутых учетных записей.

Атаки с заполнением учетных данных включают использование информации для входа из предыдущих утечек данных для компрометации учетной записи, владельцы которой повторно используют одни и те же учетные данные для входа на нескольких веб-сайтах.

Родственные бренды The North Face, принадлежащие VF Corporation, включают Altra, Dickies, Eastpak, Ice Breaker, Kipling, Napapijri, Supreme, Timberland и Vans. В 2019 году компания заработала 2 миллиарда долларов из 4 миллиардов долларов в отрасли, что сделало ее одним из лидеров рынка в сегменте одежды для активного отдыха.

Атака с заполнением учетных данных The North Face раскрыла личную информацию и информацию о покупках

Компания по производству одежды North Face остановила атаку 19 августа после обнаружения необычной активности 11 августа, хотя атака началась 26 июля 2022 года.

The North Face установила, что злоумышленники получили доступ к информации об учетных записях клиентов почти 200 000 пользователей. Детали, просочившиеся в результате атаки с заполнением учетных данных, включают полное

имя пользователя, номер телефона, пол, дату создания учетной записи, историю покупок, адреса для выставления счетов и доставки, а также баллы лояльности.

Однако злоумышленники не получили доступ к номерам кредитных карт, срокам действия и CVV, поскольку компания не хранит эту информацию.

«Мы не храним копии данных платежной карты на thenorthface.com. Мы сохраняем только «токен», связанный с вашей платежной картой, и только наш сторонний процессор платежных карт хранит данные платежной карты», — говорится в уведомлении об утечке данных.

Кроме того, The North Face объяснила, что сохраненные токены платежных карт нельзя использовать для совершения покупок на любом другом веб-сайте, кроме thenorthface.com.

Впоследствии компания приняла дополнительные меры, удалив существующие платежные токены, чтобы предотвратить злоупотребления. Таким образом, клиенты должны повторно авторизовать свои кредитные карты, чтобы совершать покупки на веб-сайте.

Пол Бишофф, защитник конфиденциальности в Comparitech, предупредил, что злоумышленники не остановятся на The North Face: «Если у вас есть учетная запись North Face и у нее есть пароль, такой же, как у других учетных записей, вы должны немедленно изменить их все».

Пользователи должны сбросить пароль любой учетной записи, которая использует учетные данные для входа в систему со скомпрометированными учетными записями на thenorthface.com. Кроме того, им следует сохранять бдительность в отношении фишинговых атак, направленных на кражу личной информации путем выдачи себя за сотрудников The North Face с использованием утекшей информации.

Пользователи также должны избегать отправки учетной записи, платежа и личной информации лицам, запрашивающим такие данные по электронной почте, текстовым сообщениям или в социальных сетях. Законные компании определили процессы сбора этой информации на своих веб-сайтах и почти не полагаются на электронную почту, текстовые сообщения или социальные сети.

По словам Уриэля Маймона, руководителя отдела новых продуктов в Human Security, атака с заполнением учетных данных North Face будет иметь каскадный эффект на другие учетные записи.

«Мы должны ожидать, что учетные данные, украденные из The North Face, вскоре будут протестированы в других приложениях, которые мы используем для обеспечения нашей повседневной жизни», — сказал Маймон. «Поэтому важно, чтобы пользователи приложений и владельцы сайтов усложняли и удорожали киберпреступникам использование информации, чтобы нарушить цикл атак».

«В 2021 году число злонамеренных попыток входа в общее количество входов в систему увеличилось, достигнув ошеломляющих 93,8% всех попыток входа в систему в августе, что на 8% больше, чем пик 2020 года», — сказал он.

Признаки основной проблемы безопасности

Этот инцидент знаменует собой второй раз, когда The North Face сбрасывала пароли после аналогичной атаки с заполнением учетных данных в 2020 году.

«Мы настоятельно рекомендуем вам не использовать тот же пароль для своей учетной записи на thenorthface.com, который вы используете на других веб-сайтах, потому что, если один из этих других веб-сайтов будет взломан, ваш адрес электронной почты и пароль могут быть использованы для доступа к вашей учетной записи на thenorthface.com.», — сообщила компания своим клиентам в 2020 году.

Компания по производству одежды не раскрыла источник украденных данных, использованных в недавней атаке с подменой учетных данных. В 2020 году компания сообщила, что злоумышленники получили учетные данные пользователей со стороннего веб-сайта и скомпрометировали нераскрытое количество учетных записей клиентов на thenorthface.com.

Очевидно, что атаки с заполнением учетных данных в 2020 и 2022 годах следуют схожим схемам, что указывает на основную проблему безопасности, требующую постоянного решения». ***(Alicia Hope. The North Face Credential Stuffing Attack Compromises 200,000 Accounts // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/the-north-face-credential-stuffing-attack-compromises-200000-accounts/). 16.09.2022).***

***

«American Airlines заявляет, что личная информация «очень небольшого числа» клиентов и сотрудников была скомпрометирована после того, как хакеры взломали учетные записи электронной почты некоторых сотрудников.

Авиакомпания заявила во вторник, что у нее есть признаки того, что злоумышленники злоупотребили какой-либо личной информацией.

Американец сказал, что нарушение было обнаружено в июле. Авиакомпания отказалась сообщить, как именно скольким людям была раскрыта их личная информация, или характер этой информации.

«American Airlines известно о фишинговой кампании, которая привела к несанкционированному доступу к ограниченному количеству почтовых ящиков членов команды», — заявил официальный представитель США Кертис Блессинг. «В этих учетных записях электронной почты содержалось очень небольшое количество личной информации клиентов и сотрудников.

Блессинг сказал, что американец вводит «дополнительные технические меры безопасности, чтобы предотвратить повторение подобного инцидента в будущем».

American базируется в Форт-Уэрте, штат Техас». ***(Hackers accessed data on some American Airlines customers // Tech Xplore (https://techxplore.com/news/2022-09-hackers-accessed-american-airlines-customers.html). 20.09.2022).***

***

«Хакеры получили доступ к системам Samsung в США и украли информацию о клиентах, заявил в пятницу гигант мобильной связи. Нарушение кибербезопасности произошло в конце июля, а к 4 августа Samsung обнаружила, что информация о клиентах была украдена.

По словам Samsung, хакеры не получили доступа к номерам социального страхования, номерам кредитных или дебетовых карт. Затронутая информация включала имена, контактную и демографическую информацию, дату рождения и

информацию о регистрации продукта. В Samsung также отметили, что потребительские устройства в этом инциденте не пострадали, и клиенты могут продолжать использовать продукты и услуги Samsung в обычном режиме.

Samsung не сразу ответила на вопросы о том, сколько клиентов пострадало.

«Мы предприняли действия для защиты пострадавших систем, привлекли ведущую стороннюю фирму по кибербезопасности и координируем свои действия с правоохранительными органами», — говорится в кратком уведомлении компании, размещенном в Интернете.

Samsung также заявила, что напрямую связалась с пострадавшими клиентами по этому поводу. Если компания обнаружит других пострадавших клиентов, она уведомит их соответствующим образом…» ***(Stephanie Condon. Hackers gained access to Samsung customer data // ZDNET (https://www.zdnet.com/article/hackers-gained-access-to-samsung-customer-data/). 02.09.2022).***

***

«В прошлом году число случаев несанкционированного доступа к личной информации (включая хакерские атаки) увеличилось на 159%, а количество нарушений, связанных с неправомерным использованием компьютеров, в целом увеличилось на 89%. В ответ на эту растущую угрозу правительство Великобритании обратилось с запросом о предоставлении информации, запрашивая мнения о «потенциальном» вмешательстве правительства.

В своем министерском предисловии (теперь бывший) министр внутренних дел Прити Патель объясняет, что «[в] его работе будут изучаться меры по снижению нагрузки на граждан в отношении кибербезопасности, включая применение организациями принципов безопасности по умолчанию для защиты учетных записей пользователей и Информация. Он также рассмотрит вопрос о том, следует ли дополнить требования законодательства о защите данных, чтобы гарантировать, что поставщики онлайн-услуг и учетных записей, а также обработчики и держатели персональных данных граждан Великобритании несут надлежащую и соразмерную степень ответственности за требуемую защиту данных. и доступ к нему».

Запрос информации является первым этапом общественных консультаций правительства по его программе «Киберобязанность защищать» (рабочее название). Программа направлена на снижение бремени кибербезопасности для граждан и снижение вреда для граждан от несанкционированного доступа и связанного с этим вреда.

Что включает в себя запрос информации и кто должен на него ответить?

Правительство Великобритании запрашивает мнения организаций, предприятий и частных лиц по следующим вопросам:

Риски, связанные с несанкционированным доступом к онлайн-аккаунтам и персональным данным граждан Великобритании.

Действия, предпринимаемые в настоящее время для решения проблемы.

Действия, которые следует предпринять для решения проблемы, и ответственность за выполнение этих действий.

В частности, он ищет респондентов, которые думают о том, как вмешательство правительства может помочь снизить кибербремя, с которым сталкиваются

граждане, и побудить организации делать больше для защиты учетных записей и личных данных пользователей. Он также приветствует ответы предприятий и отрасли о том, как им помочь лучше понять риски, с которыми они и их клиенты сталкиваются, и как их снизить. Наконец, в ходе телеконференции запрашиваются мнения о том, какие меры можно было бы принять для смягчения этих угроз и снижения нагрузки на пользователя в отношении безопасности входа в систему.

Следить за предложениями по безопасности?

После этого запроса информации правительство заявило, что оно будет работать с поставщиками услуг и другими ключевыми заинтересованными сторонами для разработки предложений по соответствующим мерам безопасности, которые могли бы реализовать поставщики онлайн-услуг и учетных записей, а также организации, обрабатывающие персональные данные. Целью этого будет обеспечение лучшей защиты учетных записей пользователей и их личных данных от атак. В предложениях также будут рассмотрены положения, обеспечивающие соблюдение этих мер.

По мнению правительства, это будет означать «изучение дополнения текущего подхода к защите данных в соответствии с Законом о защите данных и GDPR с более глубоким пониманием и учетом риска для отдельных лиц, связанного с компрометацией их данных, хранящихся в организациях». Как это будет выглядеть на практике, еще предстоит увидеть, хотя правительство признает, что любые новые предложения должны дополнять существующие обязательства. Он также признает, что уже предпринимаются определенные шаги, чтобы попытаться решить некоторые проблемы, связанные с этим. Например, законопроект о безопасности продуктов и телекоммуникационной инфраструктуре, который в настоящее время находится на рассмотрении парламента, направлен на ужесточение защиты паролей…». ***(Natalie Donovan. ORGANISATIONS COULD FACE NEW SECURITY REQUIREMENTS UNDER 'CYBER DUTY TO PROTECT' PLANS? // Slaughter and May (https://thelens.slaughterandmay.com/post/102hwnj/organisations-could-face-new-security-requirements-under-cyber-duty-to-protect). 08.09.2022).***

***

«Атаки с заполнением учетных данных стали настолько распространенными в первом квартале 2022 года, что в некоторых странах трафик превысил трафик законных попыток входа в систему от обычных пользователей.

Этот тип атаки использует преимущество «повторного использования пароля», что является плохой практикой использования одних и тех же пар учетных данных (имя пользователя и пароль) на нескольких сайтах.

После утечки или перебора учетных данных с одного сайта злоумышленники выполняют атаку с заполнением учетных данных, которая пытается использовать те же учетные данные, полученные в результате утечки, на других сайтах для получения доступа к учетным записям пользователей.

Как недавно предупредило ФБР, объемы этих атак растут благодаря легкодоступным агрегированным спискам утекших учетных данных и

автоматизированным инструментам, предоставленным киберпреступникам, позволяющим им тестировать пары на многих сайтах.

Okta сообщает, что в 2022 году ситуация ухудшилась, поскольку компания по управлению идентификацией и доступом зафиксировала более 10 миллиардов случаев заполнения учетных данных на своей платформе за первые 90 дней 2022 года.

Это число составляет примерно 34% от общего трафика аутентификации, а это означает, что треть всех попыток являются злонамеренными и мошенническими.

При рассмотрении с географической точки зрения наихудшими случаями являются Юго-Восточная Азия и Соединенные Штаты, где трафик с заполнением учетных данных постоянно превосходил обычные попытки входа в систему на протяжении первого квартала 2022 года.

Поскольку большинство этих атак следуют «взрывному» подходу, когда за короткое время проверяется большое количество учетных данных, затронутые платформы выдерживают внезапные скачки нагрузки до десяти раз.

Примером в отчете Окты является атака, длившаяся почти два месяца и завершившаяся в январе 2022 года.

Диаграмма нагрузки показывает, насколько разрушительными могут быть эти атаки для онлайн-платформ, создавая значительную нагрузку на их инфраструктуру управления идентификацией, вызывая задержку и ухудшая работу обычных пользователей.

Окта сообщает, что с точки зрения того, какие отрасли были атакованы больше всего, большинство попыток было направлено против розничной торговли/электронной коммерции. Значительные объемы атак были также зарегистрированы против образования, энергетики, финансовых услуг и программного обеспечения/SaaS.

Недавним примером атаки с использованием учетных данных на платформу электронной коммерции является атака на клиентов North Face, в результате которой было скомпрометировано около 200 000 учетных записей в интернет-магазине бренда.

Защита от атак с подменой учетных данных в основном является обязанностью онлайн-платформ, которые должны использовать проверки по отпечаткам пальцев, участвовать в проактивной проверке учетных данных, использовать системы обнаружения прокси и внедрять «теневой бан» для подозрительных учетных записей.

С точки зрения пользователей, использование многофакторной аутентификации и установка уникальных и надежных паролей для всех ваших сетевых учетных записей обеспечивает достаточную защиту от большинства угроз этого типа.

Однако, как видно из недавних атак MFA Fatigue, злоумышленники нашли способы обойти MFA с помощью социальной инженерии. Поэтому организациям важно должным образом защитить MFA с помощью сопоставления номеров и порогов попыток проверки подлинности». ***(Bill Toulas. Okta: Credential stuffing accounts for 34% of all login attempts // Bleeping Computer®***

(https://www.bleepingcomputer.com/news/security/okta-credential-stuffing-accounts-for-34-percent-of-all-login-attempts/). 21.09.2022).

***

«Фахівці з кібербезпеки з'ясували, що браузери Google Chrome і Microsoft Edge збирають дані користувача незвичайним чином.

Виявилося, що вбудовані функції перевірки орфографії у браузерах Google Chrome та Microsoft Edge передають Google та Microsoft особисті дані користувачів і в деяких випадках навіть паролі.

Залежно від відвідуваного веб-сайту, ці форми можуть включати адресу електронної пошти, дату народження, контактну інформацію, банківську інформацію, платіжну інформацію тощо.

Тішить лише те, що в браузерах є можливість відключення функцій перевірки орфографії». ***(Браузери Google Chrome і Microsoft Edge крадуть дані користувача під час перевірки орфографії // iLenta (https://ilenta.com/uk/news/internet/internet_995.html). 21.09.2022).***

***

«Британська компанія з кібербезпеки Comparitech опублікувала звіт, у якому проаналізовано використання систем відеоспостереження у 150 найбільш густонаселених містах світу. Виявилося, що найактивніше стежить за своїми громадянами комуністичний уряд Китаю.

У звіті згадується зроблений кілька років тому прогноз британського постачальника інформаційних послуг IHS Markit про те, що до кінця 2021 року у світі буде близько 1 мільярда камер спостереження, з них 54 % — у Китаї, тобто близько 540 мільйонів камер спостереження, що еквівалентно 372 камерам на кожну тисячу жителів КНР.

Це досить стримана оцінка. Пізніше компанія IHS Markit повідомляла, що в Китаї встановлено 626 мільйонів камер спостереження, тобто 432,2 камери на тисячу осіб.

Крім Китаю, велику кількість камер спостереження встановлено в індійському місті Індуар. Там у середньому розташовано 62,52 камери на тисячу осіб. В інших країнах камер менше: у Лондоні (Великобританія) — 13,35 на тисячу осіб, у Лос-Анджелесі (США) — 8,77 на тисячу осіб, у найбільш густонаселеному місті світу Токіо (Японія) — лише 1,06 камер на тисячу осіб.

Якщо рахувати за щільністю розташування камер, то лідерами також є китайські міста. Список очолило місто Шеньчжень провінції Гуандун із середнім показником у 6220 камер спостереження на квадратну милю (2,59 квадратних кілометра). За ним ідуть міста Ухань провінції Хубей — 5429 камер на квадратну милю; Шанхай — 4343 камер; Циндао провінції Шаньдун — 3470 камер на квадратну милю.

За межами Китаю найбільша щільність камер у Делі (Індія) — 1446 на квадратну милю. За ним ідуть Сеул (Південна Корея) — 333 камери на квадратну милю; Москва (Росія) — 220 на квадратну милю; Нью-Йорк (США) — 187 на квадратну милю; Осака (Японія) — менше ніж 6 на квадратну милю.

На додаток до великої кількості та високої щільності встановлені китайські камери спостереження також дуже функціональні. У вересні 2019 року китайські вчені запустили хмарну систему камер із роздільною здатністю в 500 мегапікселів, яка дає змогу робити як фотографії, так і відео.

За словами творців цієї системи, вона має роздільну здатність, що вчетверо перевищує межу людського ока, і якщо за її допомогою зробити, наприклад, панорамну фотографію стадіону з десятками тисяч людей, то можна буде розглянути деталі обличчя кожної людини. У поєднанні з технологіями штучного інтелекту, такими як розпізнавання облич, конкретний об'єкт можна знайти в одну мить.

Чимало людей вважають, що подібне відеоспостереження може поліпшити роботу правоохоронних органів і запобігти злочинності. Однак британська дослідницька компанія Comparitech виявила, що це не так. Співробітники компанії порівняли кількість камер спостереження з індексом злочинності та дійшли висновку, що більша кількість камер не впливає на рівень злочинності.

Тоді навіщо влада Китаю витрачає такі великі ресурси на ці проєкти? Згідно з інтернет-журналом Bitter Winter, який висвітлює ситуацію з правами людини в Китаї, кінцевою метою компартії Китаю є створення повної бази даних, що дасть змогу органам безпеки відстежувати, аналізувати і контролювати кожного жителя країни в режимі реального або близького до реального часу. Тобто йдеться про створення за допомогою просунутих систем спостереження «цифрової авторитарної держави».

У квітні нинішнього року агентство «Рейтер» повідомило, що в результаті аналізу понад 50 документів, що перебувають у відкритому доступі, з'ясувалося, що за останні чотири роки десятки китайських організацій придбали програму з функцією штучного інтелекту під назвою «одна людина, один файл» (one person, one file). У документах ідеться про те, що звичайна система моніторингу може тільки збирати дані, але класифікувати їх необхідно вручну, а програма "одна людина, один файл" може сама аналізувати величезні дані і використовувати складні алгоритми для створення користувацьких файлів для кожної людини. Профілі автоматично оновлюються в міру того, як програма отримує нові дані. Ця система також має можливості самонавчання для оптимізації точності створення файлів у міру збільшення обсягу даних». ***(Британська компанія з кібербезпеки: Більша частина камер спостереження у світі розташовані в Китаї // Велика Епоха (https://www.epochtimes.com.ua/novyny-suspilstva/brytanska-kompaniya-z-kiberbezpeky-bilsha-chastyna-kamer-sposterezhennya-u-sviti-roztashovani-v-146216). 19.09.2022).***

***

«Исследование, проведенное торговым органом Audiovisual Anti-Piracy Alliance (AAPA) в отношении вредоносных программ и аудиовизуального пиратства, выявило значительные риски для европейских потребителей.

Независимый отчет, подготовленный профессором Полом Уоттерсом, почетным профессором криминологии и исследований в области безопасности в Университете Маккуори, Австралия, показывает, что в течение 71 секунды после нажатия на пиратский веб-сайт потребитель сталкивается с риском потери личности,

кражи учетных данных и требования выкупа. Риск заражения вредоносным ПО еще выше для потребителей, получающих доступ к пиратскому контенту через приложения, с вероятностью 57%, что он поставляется со встроенным вредоносным ПО.

Представляя отчет от имени профессора Уоттерса на семинаре Международного колледжа исследователей интеллектуальной собственности (IIPCIC) по цифровому пиратству в Сеуле, Марк Малреди, сопрезидент AAPA и вице-президент Irdeto по кибербезопасности, сказал: «В этом отчете освещаются очень реальные скрытые риски для потребителей, получающих доступ к пиратскому контенту, и компаний, которые их используют. В отчете также указывается, что действующего законодательства ЕС недостаточно для смягчения этих рисков, которые требуют немедленного внимания со стороны политиков и законодателей. Предстоящий Закон ЕС о киберустойчивости предоставляет одну возможность усилить нашу защиту от вредоносных программ. В своих диалогах с магазинами приложений AAPA также будет призывать хостов проявлять более строгую должную осмотрительность перед запуском приложения».

«Посещая пиратский поток или загружая пиратское приложение, потребители подвергаются крайнему риску заражения вредоносным ПО», — предупредил Уоттерс. «Исходя из этого исследования, создается впечатление, что у киберпреступников появляется новая тенденция использовать потребителей для доставки полезной нагрузки в корпоративную сеть через виртуальную частную сеть. Просмотр пиратского стрима в обеденное время не только сэкономит несколько долларов, но и может привести к краху вашей компании из-за целенаправленной вредоносной атаки». ***(Colin Mann. Study: Malware risks from AV piracy // Advanced Television Ltd. (https://advanced-television.com/2022/09/20/study-malware-risks-from-av-piracy/). 20.09.2022).***

***

«…Представители правительства Австралии оспорили утверждения руководителей Optus о том, что кибератака была осуществлена изощренным злоумышленником.

О’Нил назвал это «простым взломом», добавив, что почти у половины всех взрослых австралийцев личные данные были скомпрометированы в результате атаки.

«У нас не должно быть телекоммуникационного провайдера, который фактически оставляет окно открытым для кражи данных такого рода», — сказал О’Нил.

По данным федеральных властей, из почти 10 миллионов человек, чьи личные данные были скомпрометированы в результате атаки, у 2,8 миллиона человек были украдены обширные личные данные.

«На самом деле это составляет 100 точек проверки личности, поэтому возможности для кражи личных данных и мошенничества весьма значительны, особенно для этих 2,8 миллионов австралийцев», — сказал О’Нил.

Федеральная полиция Австралии заявила, что работает с Optus и властями Великобритании, США, Европы и Африки, чтобы выявить виновных и защитить

австралийцев от мошенничества с личными данными в результате атаки». ***(Matt Kapko. Australia's telecom giant Optus avoids ransom demand as attacker reverses course // Industry Dive (https://www.cybersecuritydive.com/news/optus-ransomware-retracted/632763/). 27.09.2022).***

***

«Социальные сети могут быть полезны для многих вещей. Он может держать вас на связи с друзьями и родственниками вдали, помочь вам найти единомышленников и предоставить доступ к ценным советам от экспертов. В конце концов, именно поэтому 4,62 миллиарда человек (или 58,4% населения мира) пользуются социальными сетями. Но если вы владелец бизнеса, такая активность в социальных сетях может представлять серьезную угрозу кибербезопасности…

Фактически, в период с ноября 2020 года по октябрь 2021 года во всем мире произошло почти 24 000 инцидентов кибербезопасности, которые затронули большие и малые предприятия. Но чем же так опасны эти популярные платформы? Вот три причины.

Легкий доступ к сотрудникам

В попытках получить доступ к информации компании через ее сотрудников нет ничего нового. Эта практика называется социальной инженерией. До социальных сетей преступник находил кого-то, кто работал в компании, звонил ему и притворялся генеральным директором, запрашивая документ или информацию, которые он потерял. Затем, поверив звонившему, сотрудник отправлял личную информацию, открывая бизнес для серьезной утечки данных.

Сегодня арендаторы социальной инженерии те же; просто механизмы изменились. Вместо использования телефона преступник может использовать социальные сети и Интернет. Как? Ну, все, что им нужно сделать, это создать профиль на платформе (т.е. LinkedIn) и друзей. Когда есть взаимные связи, преступник выглядит более законным. Это повышает уровень доверия, одновременно устраняя тот внутренний инстинкт, который у вас может быть по телефону или лично. Тогда они могут легко связаться и запросить информацию о компании.

Ни один сотрудник не передаст информацию незнакомцу, который просто подойдет к нему и попросит информацию о компании. Но социальные сети убирают этот инстинкт благодаря виртуальным связям. Преступнику легче манипулировать кем-то, так как отсутствует элемент «лицом к лицу».

Расширенные возможности

Хакеры используют термин «поверхность атаки», когда описывают, насколько легкой будет цель. Опять же, вы можете понять, как это работает, взглянув на классическое криминальное поведение. Например, если грабитель пытается украсть что-то из дома, он будет смотреть, сколько там разных входов — дверей, окон, гаража и т. д. Количество точек доступа увеличивается по мере увеличения количества окон, световых люков и т. д.., увеличивается.

Социальные сети очень похожи на преступников, стремящихся получить доступ к информации компании. Поскольку почти каждый сотрудник компании

присутствует в Интернете, все они становятся возможными точками входа, увеличивая поверхность атаки. На самом деле, он дует настежь.

Например, если хакер хочет взломать P&G, он может войти в LinkedIn, найти P&G и найти почти каждого человека, который там работает. Затем они могут найти страницы этих сотрудников в TikTok, Instagram и Facebook, чтобы узнать об их друзьях и интересах. Эта информация может помочь им связаться с этими людьми и в конечном итоге получить информацию. Поскольку поверхность атаки настолько велика, это можно сделать тысячи раз, что увеличивает шансы преступника получить желаемую информацию.

Использование психологической слабости

К сожалению, научно доказано, что просмотр социальных сетей заставляет наш мозг выделять дофамин и серотонин. И когда вы получаете лайки или подписчиков, это увековечивает эту зависимость. К сожалению, преступник может использовать эту психологию в своих интересах.

Возвращаясь к теме социальной инженерии, связываясь с кем-то в социальных сетях — и их связи — психологически вы заставите этого человека чувствовать себя более ценным. Кто-то заинтересован в вас настолько, что хочет следить за вашими повседневными делами и интересами, верно? Это дает вам прилив дофамина и серотонина. Затем этот человек (также известный как преступник) комментирует или лайкает определенные сообщения, подпитывая эту зависимость от социальных сетей. Со временем эта спешка приводит к доверию человека, даже если он незнакомец. Теперь жизненно важная информация может быть скомпрометирована.

В конце концов, социальные сети остаются слабым местом, даже если компания принимает все меры предосторожности, необходимые для защиты внутренней информации. Но понимание рисков, создаваемых социальными сетями — более легкий доступ к сотрудникам, увеличение площади атаки и использование психологической слабости — может помочь компаниям лучше подготовиться к утечке информации». ***(Mark Stamford. Why Social Media Is a Weak Spot for Companies' Cybersecurity // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/why-social-media-is-a-weak-spot-for-companies-cybersecurity/). 26.09.2022).***

***

«2022 год обещает быть чрезвычайно успешным для киберпреступников. Утечки данных накапливаются в беспрецедентных количествах, в результате чего все больше и больше информации попадает в руки злоумышленников. Кибератаки в этом году затронули крупных игроков, таких как Cash App и Красный Крест, а также более мелкие компании по всему миру. Даже небольшие утечки данных играют свою роль в более широком ландшафте скомпрометированных учетных данных. Технологии и инструменты, от которых зависит безопасность нашего бизнеса, должны быть достаточно гибкими, чтобы учитывать эту постоянно меняющуюся среду.

Поэтому удивительно, что Microsoft Azure AD Password Protection этого не делает. Пользователям рекомендуется полагаться на функцию защиты паролей Microsoft, чтобы обнаруживать и блокировать использование известных слабых паролей и их вариантов. Тем не менее, он не проверяет какие-либо доступные списки

скомпрометированных паролей или подавляющее большинство паролей из черного списка при сканировании слабых паролей.

Как объясняет Microsoft, «глобальный список запрещенных паролей основан на текущих результатах телеметрии и анализа безопасности Azure AD». Это означает, что они собирают данные только о предыдущих атаках на свою инфраструктуру. Тем временем Microsoft игнорирует все свободно доступные данные о прошлых взломах. Но можете поспорить, хакеры не игнорируют это. Кроме того, Azure AD Password Protection использует минималистский подход к внесению в черный список общих словарных слов.

Все это создает множество пробелов в защите паролей для любой компании, которая ожидает, что Azure AD Password Protection защитит их системы от этих легко эксплуатируемых уязвимостей.

Угроза взлома паролей данных

Мы никогда не сможем избежать того факта, что пользователи — люди, совершающие человеческие ошибки. Нам, людям, нравится то, что нам знакомо. Мы помним то, что нам знакомо. Когда дело доходит до паролей, это означает, что мы снова и снова возвращаемся к одним и тем же хорошо известным комбинациям символов и цифр. Когда пароли раскрываются при утечке данных, а пользователи продолжают использовать эти скомпрометированные учетные данные в ваших системах без вашего ведома, ваша организация становится уязвимой. Преступники теперь имеют больше шансов проникнуть в ваши системы с помощью простых и широко распространенных методов взлома, таких как подмена учетных данных и распыление паролей.

Настойчиво новости о кибербезопасности представляют собой список последних и самых серьезных утечек данных нашего времени. Стоимость этих атак стремительно растет. В отчете IBM «Стоимость утечки данных за 2022 год» говорится, что потери все еще растут, увеличившись в среднем с 4,24 миллиона долларов за утечку в 2021 году до 4,35 миллиона долларов в 2022 году. Эти цифры не могут даже объяснить эффект домино первоначальных кибератак и затрат организаций, которые впоследствии были взломаны с помощью этих украденных учетных данных. Но мы знаем, что украденные или скомпрометированные учетные данные стали причиной 19% взломов в этом году, согласно отчету IBM. Если организации применяют более активный подход к безопасности паролей и происходит взлом, это обходится жертве в среднем на 3,05 миллиона долларов меньше. Организации с архитектурой нулевого доверия также экономят. В этих случаях нарушения обходятся в среднем на 1 миллион долларов меньше.

Как защита паролей Azure AD обходит очевидное

Руководство по паролям NIST 800-63B говорит нам: «При обработке запросов на установление и изменение запомненных секретов верификаторы ДОЛЖНЫ сравнивать предполагаемые секреты со списком, который содержит значения, которые, как известно, обычно используются, ожидаются или скомпрометированы». В частности, сюда входят скомпрометированные пароли, полученные в результате предыдущих взломов, а также словарные слова (и их варианты), повторяющиеся или последовательные символы и контекстно-зависимые слова.

Удивительно, но решение Microsoft для паролей не пытается предотвратить использование паролей, которые уже были раскрыты в предыдущих взломах, несмотря на то что говорится в рекомендациях NIST. Их глобальный список запрещенных паролей также не включает все общеупотребительные словарные слова. Он построен на чрезвычайно усеченном списке, состоящем всего из 500 наиболее часто используемых паролей и их вариантов (например, слов с заменой символов). В собственных рекомендациях Microsoft говорится, что надежный пароль — это «не слово, которое можно найти в словаре, или имя человека, персонажа, продукта или организации», но их собственный инструмент не следует этому совету.

Защита паролей Azure AD не помешает пользователю создать пароль из тысяч распространенных английских слов, не говоря уже о распространенных словарных словах других языков. Сосредоточив внимание на минимальном списке паролей базовых терминов, защита паролей Azure AD также не учитывает региональные различия в популярных паролях. Они предлагают возможность создать собственный запрещенный список, но это больше для того, чтобы предприятия могли включать такие вещи, как названия брендов, а не пытаться охватить все, что Microsoft упускает. Потрясающе (а может, и не так уж поразительно) 44 миллиона. Учетные записи Microsoft Azure AD и Microsoft Services использовали скомпрометированные пароли. Похоже, что многие слишком сильно полагаются на эту функцию защиты паролем, оставляя свои учетные записи и системы открытыми для взлома киберпреступниками. Такие инструменты, как Enzoic для Active Directory, позволяют невероятно легко заполнить эти пробелы в безопасности, автоматически сопоставляя ваши пароли с недавними утечками данных и защищая скомпрометированные учетные данные и занесенные в черный список словарные слова (все они) от ваших систем. Когда так легко укрепить свою безопасность, зачем соглашаться на меньшее?» ***(The Risks Azure AD Password Protection Ignores: Compromised and Blacklisted // Techstrong Group Inc. (https://securityboulevard.com/2022/09/the-risks-azure-ad-password-protection-ignores-compromised-and-blacklisted/). 28.09.2022).***

***

«В ходе недавнего аудита Управление генерального инспектора HHS (OIG) обнаружило, что Национальные институты здравоохранения (NIH) не выполнили надлежащих требований, чтобы гарантировать, что его гранты имеют средства защиты кибербезопасности на основе рисков для защиты конфиденциальных данных.

«Национальные институты здравоохранения (NIH) ежегодно инвестируют более 30 миллиардов долларов в медицинские исследования для американского народа. Более 80 процентов финансирования NIH предоставляется через почти 50 000 конкурсных грантов различным исследовательским учреждениям во всех 50 штатах и во всем мире», — говорится в отчете.

«Таким образом, защита данных и средства контроля безопасности, защищающие исследовательскую деятельность, финансируемую из федерального бюджета, имеют большое значение как для HHS, так и для федерального правительства».

Компания CliftonLarsonAllen LLP (CLA) провела аудит от имени OIG. CLA провела интервью с официальными лицами Национального института здоровья, проверила адекватность, мониторинг и правоприменение обеспечения кибербезопасности института, а также проверила средства контроля кибербезопасности получателя гранта.

ФОН

Поскольку NIH является организацией, предоставляющей гранты, она обязана соблюдать федеральные требования, чтобы обеспечить защиту своих данных на протяжении всего процесса предоставления грантов.

«Федеральные грантополучатели должны установить и поддерживать эффективный внутренний контроль, чтобы обеспечить разумную уверенность в том, что грантополучатель управляет грантом в соответствии с федеральными законами и политикой, а также условиями гранта», — говорится в отчете.

Руководство HHS по администрированию политики в отношении грантов (GPAM) требует, чтобы NIH и другие агентства HHS, предоставляющие грантовые средства, налагали на получателя гранта особые условия, соответствующие рискам, связанным с грантом.

Кроме того, действующее Заявление о политике грантов NIH (NIHGPS) содержит общие положения о безопасности данных и требует, чтобы получатели грантов не хранили исследования, поддерживаемые NIH, на портативных электронных устройствах и ограничивали доступ с помощью защиты паролем и надлежащего контроля доступа.

РЕКОМЕНДАЦИИ И ОТВЕТ NIH

В своем анализе GPAM, NIHGPS и других политик выводы CLA показали, что NIH не учитывает соображения кибербезопасности. Например, CLA обнаружил, что у NIH «не было надлежащего процесса оценки рисков до присуждения решения, поскольку он не учитывает кибербезопасность и не включает в уведомление о присуждении специального условия, касающегося риска кибербезопасности».

По сути, текущая версия NIHGPS, с точки зрения CLA, неадекватна для обеспечения того, чтобы NIH знал о недостатках кибербезопасности из-за отсутствия мониторинга и оценок до и после присуждения награды. Сами грантополучатели несут ответственность за внедрение и поддержание безопасности данных.

Аудит показал, что положения о кибербезопасности NIHGPS слишком общие. В некоторых случаях кибербезопасность вообще не рассматривалась.

CLA рекомендовала NIH с самого начала требовать дополнительной защиты от кибербезопасности, включая соображения кибербезопасности в объявления о возможностях финансирования или условиях гранта. CLA также предложила NIH укрепить NIHGPS и его процессы до и после присуждения контракта, чтобы определить, были ли реализованы меры безопасности в области кибербезопасности.

Несмотря на эти рекомендации, ответ NIH «не указывал на согласие или несогласие» с ними.

«NIH считает пять рекомендаций закрытыми и реализованными в соответствии с существующими требованиями NIHGPS, опубликовал рекомендации

по передовой практике и опубликовал запланированное добавление заявлений о политике управления и обмена данными (DMS) в NIHGPS», — отмечается в отчете.

«Основываясь на нашем обзоре комментариев NIH, мы определили, что описанные действия не в полной мере учитывают выявленные риски кибербезопасности. Таким образом, мы утверждаем, что наши выводы и рекомендации являются точными и действительными. Мы призываем NIH выполнить наши рекомендации по усилению контроля кибербезопасности над своей программой грантов». ***(Jill McKeon. OIG Finds NIH Health Grant Program Needs Stricter Cybersecurity Controls // TechTarget, Inc. (https://healthitsecurity.com/news/oig-finds-nih-health-grant-program-needs-stricter-cybersecurity-controls). 28.09.2022).***

***

«Официальные лица подтвердили, что хакеры, которые нанесли ущерб французской больнице и украли множество данных в прошлом месяце, опубликовали личные записи пациентов в Интернете.

Киберзлоумышленники месяц назад потребовали многомиллионный выкуп от больницы Корбей-Эссонн под Парижем, но учреждение отказалось платить.

В больнице заявили, что хакеры теперь сбросили медицинские снимки и лабораторные анализы вместе с номерами пациентов из национальной безопасности.

«Я самым решительным образом осуждаю невыразимое раскрытие хакерских данных», — написал в воскресенье министр здравоохранения Франсуа Браун.

Больницы по всему миру сталкиваются с растущими атаками со стороны групп программ-вымогателей, особенно после того, как пандемия истощила ресурсы до предела.

Проблема остро стояла во Франции, где официальные лица в начале прошлого года подсчитали, что учреждения здравоохранения в среднем сталкивались с атаками каждую неделю.

Президент Эммануэль Макрон в прошлом году назвал атаки во время пандемии «кризисом внутри кризиса» и объявил о дополнительном миллиарде евро на кибербезопасность.

Во время атаки в прошлом месяце больница Корбей-Эссонн закрыла свои службы экстренной помощи и отправила многих пациентов в другие учреждения.

В какой-то момент официальные лица заявили, что единственной технологией, которая все еще работает, является телефон.

Вместо того, чтобы продавать огромное количество данных, хакер выложил хотя бы часть из них для загрузки в «даркнет» — скрытую часть Интернета, для доступа к которой требуется специальное программное обеспечение.

Аналитики говорят, что это похоже на тактику оказания давления на больницу, хотя французское законодательство запрещает государственным учреждениям платить выкуп.

Исследователь кибербезопасности Дэмиен Бэнкал, который обнаружил утечку и видел файлы, сказал AFP, что опасается, что другие преступники теперь будут запускать мошенничество с данными, которые уже были разглашены.

В ответ на утечку в выходные больница строго ограничила доступ к своим системам и призвала пациентов быть предельно бдительными при получении электронных писем, текстовых сообщений или телефонных звонков». ***(Hackers leak French hospital patient data in ransom fight // Tech Xplore (https://techxplore.com/news/2022-09-hackers-leak-french-hospital-patient.html). 26.09.2022).***

***

Кібербезпека Інтернету речей

«За словами міністра клімату та енергетики Нідерландів Роба Джеттена, державне агентство радіозв'язку Нідерландів почало розслідування того, чи становлять фотоелектричні інвертори загрозу кібербезпеці електроенергетичної системи Нідерландів.

У документі, опублікованому на веб-сайті парламенту Нідерландів, Джеттен сказав, що пристрої Інтернету речей, такі як фотоелектричні інвертори, можуть становити небезпеку для електромережі.

«Щоб знизити ризики, пов'язані з цими пристроями, ми приділяємо особливу увагу запобіганню, підвищенню обізнаності та додатковому законодавству, яке робить продукти більш стійкими до цифрових атак», — сказав він. «Агентство радіозв'язку розпочне переговори з відповідними виробниками про те, як покращити кібербезпеку».

Голландський хакер, відомий як Jelle Ursem, нещодавно отримав доступ до фотоелектричних систем, керованих за допомогою інструменту моніторингу, розробленого китайським виробником Solarman, повідомляє голландське ЗМІ Tweakers.

«Хакер зміг переглянути особисті дані голландських клієнтів, створити нових клієнтів і видалити існуючих користувачів», — повідомили Tweakers. «Він також зміг дізнатися, скільки електроенергії генерують сонячні панелі клієнтів, використовуючи GPS-координати, а також завантажити, налаштувати та перезавантажити прошивку інвертора».

Представник Solarman сказав, що проблему було вирішено без будь-якого реального впливу на порушені фотоелектричні системи». ***(У Нідерландах почалося розслідування щодо кібербезпеки фотоелектричних інверторів після злому // Журнал "Україна Електро" (https://ua-electro.com/u-niderlandax-pochalosya-rozsliduvannya-shhodo-kiberbezpeki-fotoelektrichnix-invertoriv-pislya-zlomu/). 06.09.2022).***

***

«Искусственный интеллект играет все более важную роль в кибербезопасности — как во благо, так и во вред. Организации могут использовать новейшие инструменты на основе ИИ для более эффективного обнаружения угроз и защиты своих систем и ресурсов данных. Но

киберпреступники также могут использовать эту технологию для проведения более изощренных атак.

Рост числа кибератак способствует росту рынка продуктов безопасности на основе ИИ. В отчете Acumen Research and Consulting за июль 2022 года говорится, что мировой рынок составлял 14,9 миллиарда долларов в 2021 году и, по оценкам, достигнет 133,8 миллиарда долларов к 2030 году.

Растущее число атак, таких как распределенный отказ в обслуживании (DDoS) и утечка данных, многие из которых обходятся пострадавшим организациям чрезвычайно дорого, вызывают потребность в более сложных решениях.

Согласно отчету, еще одним фактором роста рынка стала пандемия Covid-19 и переход на удаленную работу. Это вынудило многие компании уделить повышенное внимание кибербезопасности и использованию инструментов на основе ИИ для более эффективного обнаружения и предотвращения атак.

Ожидается, что в будущем такие тенденции, как растущее внедрение Интернета вещей (IoT) и увеличение числа подключенных устройств, будут способствовать росту рынка, говорится в отчете Acumen. Растущее использование облачных сервисов безопасности также может предоставить возможности для новых применений ИИ для кибербезопасности.

Повышение безопасности ИИ

Среди типов продуктов, использующих ИИ, — антивирусы/антивредоносные программы, предотвращение потери данных, обнаружение мошенничества/противодействие мошенничеству, управление идентификацией и доступом, система обнаружения/предотвращения вторжений, а также управление рисками и соответствием требованиям.

До сих пор использование ИИ для кибербезопасности было несколько ограничено. «Компании до сих пор не передают свои программы кибербезопасности ИИ», — сказал Брайан Финч, соруководитель практики кибербезопасности, защиты данных и конфиденциальности в юридической фирме Pillsbury Law. «Это не означает, что ИИ не используется. Мы видим, как компании используют ИИ, но в ограниченных масштабах», в основном в контексте таких продуктов, как фильтры электронной почты и инструменты идентификации вредоносных программ, которые каким-то образом используют ИИ.

«Самое интересное, что мы видим, что инструменты поведенческого анализа все чаще используют ИИ», — сказал Финч. «Под этим я подразумеваю инструменты, анализирующие данные, чтобы определить поведение хакеров, чтобы увидеть, есть ли закономерность в их атаках — время, метод атаки и то, как хакеры перемещаются внутри систем. Сбор такой информации может быть очень ценным для защитников».

По словам вице-президента по исследованиям Марка Драйвера, в недавнем исследовании исследовательская компания Gartner опросила около 50 поставщиков систем безопасности и обнаружила среди них несколько моделей использования ИИ.

«В подавляющем большинстве они сообщили, что первой целью ИИ было «удалить ложные срабатывания», поскольку одной из основных проблем аналитиков безопасности является фильтрация сигнала из шума в очень больших наборах данных», — сказал Драйвер. «ИИ может обрезать это до разумного размера, что

намного точнее. В результате аналитики могут работать умнее и быстрее, чтобы устранять кибератаки».

По словам Драйвера, в целом ИИ используется для более точного обнаружения атак, а затем для определения приоритетов реагирования в зависимости от реального риска. И это позволяет автоматически или полуавтоматически реагировать на атаки и, наконец, обеспечивает более точное моделирование для прогнозирования будущих атак. «Все это не обязательно исключает аналитиков из цикла, но делает их работу более гибкой и более точной при столкновении с киберугрозами», — сказал Драйвер.

Добавление к киберугрозам

С другой стороны, злоумышленники также могут использовать ИИ несколькими способами. «Например, ИИ можно использовать для выявления шаблонов в компьютерных системах, которые выявляют слабые места в программном обеспечении или программах безопасности, что позволяет хакерам использовать эти недавно обнаруженные слабости», — сказал Финч.

В сочетании с украденной личной информацией или собранными данными из открытых источников, такими как сообщения в социальных сетях, киберпреступники могут использовать ИИ для создания большого количества фишинговых электронных писем для распространения вредоносных программ или сбора ценной информации.

«Эксперты по безопасности отметили, что фишинговые электронные письма, сгенерированные искусственным интеллектом, на самом деле имеют более высокие показатели открываемости — [например] заставляя возможных жертв щелкнуть по ним и, таким образом, спровоцировать атаки — чем фишинговые электронные письма, созданные вручную», — сказал Финч. «ИИ также можно использовать для создания вредоносных программ, которые постоянно меняются, чтобы избежать обнаружения автоматическими защитными инструментами».

Постоянно меняющиеся сигнатуры вредоносных программ могут помочь злоумышленникам обойти статические средства защиты, такие как брандмауэры и системы обнаружения периметра. Точно так же вредоносное ПО на основе ИИ может находиться внутри системы, собирая данные и наблюдая за поведением пользователей, пока не будет готово начать новую фазу атаки или отправить собранную информацию с относительно низким риском обнаружения. Отчасти поэтому компании переходят к модели «нулевого доверия», когда средства защиты настроены на постоянную проверку и проверку сетевого трафика и приложений, чтобы убедиться, что они не являются вредоносными…» ***(Bob Violino. Artificial intelligence is playing a bigger role in cybersecurity, but the bad guys may benefit the most // CNBC LLC. (https://www.cnbc.com/2022/09/13/ai-has-bigger-role-in-cybersecurity-but-hackers-may-benefit-the-most.html). 13.09.2022).***

***

«В то время как средняя стоимость утечки данных в 2021 году превысила 9 миллионов долларов, расчет широкомасштабной киберфизической атаки в отрасли здравоохранения остается неопределенным и непредвиденным. В

условиях международного киберконфликта и целого ряда угроз правительство США начинает проливать новый свет на растущую проблему.

Несмотря на распространение программ-вымогателей, многие заинтересованные стороны в отрасли остаются в неведении, когда дело доходит до понимания киберфизических рисков, связанных с операционными медицинскими технологиями, Интернетом медицинских вещей (IoMT) и цифровыми компонентами управления операциями и объектами.

От деловых записей до данных пациентов и диагностики, планирования, лечения, рецептов, платежей, объектов и многого другого медицинское обслуживание оцифровано. Одна тема пересекает ландшафт киберугроз медицинских технологий, устройств, больниц и государственных медицинских учреждений: путаница.

Стремление объединить множество подключенных конечных точек в «единую панель», часто вводимое без согласования политики безопасности, приводит к компромиссу между простыми в развертывании и сложными для защиты технологиями. Подобно зеркальному дому, ответственность за понимание и снижение кибер-рисков в здравоохранении трудно разграничить и часто зависит от того, кого вы спрашиваете, особенно когда речь идет о некорпоративных системах и устройствах.

IoT представляет собой двустороннее зеркало, предлагающее окно для целевых сетей и мероприятий в области медицинских технологий и здравоохранения. Жестко закодированные пароли и учетные данные подвергаются атакам, пользовательские интерфейсы от производителей взламываются, процессы управления изменениями обходят, а широко распространенные уязвимости продолжают влиять на тысячи устройств по всему миру.

Оперативные медицинские технологии, технологии IoMT и системы объектов охватывают широкий спектр машин и конфигураций, в том числе машины для диагностики и мониторинга пациентов, такие как наркозные аппараты и прикроватные мониторы, оборудование для медицинской визуализации, инсулиновые помпы, жидкостные помпы, аппараты ИВЛ и растущий список датчики, камеры, носимые устройства и средства аналитики, которые обеспечивают или сообщают о состоянии оборудования, процессов и операций.

Проблемы кибербезопасности для здравоохранения многогранны, включая уязвимые технологии, разработанные без учета безопасности, подключенные к Интернету устройства, используемые непосредственно для ухода за пациентами, а также технологии интеллектуальных зданий и автоматизированных объектов.

Как отмечает FDA, «Неспособность поддерживать кибербезопасность на протяжении всего жизненного цикла медицинского устройства может привести к нарушению функциональности, потере медицинских или личных данных, неадекватной целостности данных или распространению угроз безопасности на другие подключенные устройства или сети… вред пациенту, такой как болезнь, травма или смерть в результате несвоевременного лечения или других воздействий на доступность и функциональность медицинского устройства».

Устаревшие медицинские технологии

Устаревшие технологии в здравоохранении распространены повсеместно, их замена обходится дорого, и они могут быть использованы в результате хорошо известных тактик кибератак и растущего списка общедоступных распространенных уязвимостей и уязвимых мест (CVE). Многие работают на устаревшем программном обеспечении, таком как Windows XP и Windows 7, и имеют ограниченные механизмы для применения критических исправлений и обновлений в широко распределенных и неуправляемых развертываниях. Ресурсы и рабочая сила ограничивают возможность отслеживать, защищать и постоянно улучшать каждый компонент устаревшей медицинской технологии, используемой сегодня.

На высоком уровне производители несут ответственность за безопасность продуктов, обслуживание жизненного цикла, обнаружение уязвимостей, а также создание и распространение доступных исправлений и обновлений для постоянной защиты производимых ими устройств и технологий.

Конечные пользователи одновременно несут ответственность за отслеживание и устранение обнаруженных уязвимостей, включение функций безопасности, защиту данных при передаче и хранении, а также развертывание решений для мониторинга технологий и сетей, работающих в их организации. В то же время большинство команд и локаций не готовы вернуться к ручным операциям в течение длительного периода времени.

Интернет медицинских устройств (IoMT)

По данным Управления по санитарному надзору за качеством пищевых продуктов и медикаментов, США регулируют около 200 000 медицинских устройств, производимых более чем 18 000 компаний по всему миру. Интеллектуальные подключенные медицинские устройства охватывают как пользовательские интерфейсы (для пациентов и поставщиков медицинских услуг), так и связь между машинами через сетевое подключение.

Эти устройства, часто способные подключаться к Интернету, сопряжены с рисками, связанными с несанкционированным доступом, взломом интерфейсов входа в систему для обхода аутентификации по паролю, распределенными атаками типа «отказ в обслуживании» (DDoS) и ограниченной защитой конфиденциальной информации о пациентах.

Основной поверхностью атаки для устройств IoT являются учетные данные по умолчанию через SSH. Когда система становится целью, злоумышленник, обычно другое зараженное устройство IoT, пытается ввести в среднем сорок паролей для нескольких имен пользователей. Другие распространенные поверхности для атак этих устройств включают UPnP, HTTPS и лежащие в их основе пакеты Java и различные модификации исходного кода.

Эти системы и варианты, как правило, остаются без исправлений в течение долгого времени после выпуска исправления из-за того, что большинство устройств IoT являются безголовыми (без пользовательского интерфейса) и не настроены для автоматических обновлений без согласия пользователя с заявлением, основанным на рисках, в конце -пользовательские лицензионные соглашения.

Умные, подключенные объекты

Медицинские и медицинские операции и учреждения продолжают оцифровывать компоненты систем управления, не связанных с ИТ, — пожарную

сигнализацию и подвеску, электрические и осветительные системы, системы учета, зарядные станции для транспортных средств, ключи контроля доступа. Когда элементы управления централизованы, компании часто внедряют решения для автоматизации зданий (BAS) для подключения и автоматизации управления этими разнообразными функциями. Недостатки безопасности в BAS могут использоваться для получения доступа к учетным данным, сетям и VPN, а также к конфиденциальным данным.

В ходе недавнего исследования умного здания мы обнаружили 361 используемый незащищенный протокол, 259 открытых уязвимостей устройств и 37 открытых (незашифрованных) паролей.

Получив контроль над одним или несколькими устройствами, злоумышленники могут координировать более масштабные атаки в зависимости от уровня широкомасштабного подключения.

Кибербезопасность для операций и объектов, возможно, наиболее важна в больницах, где собирается критическое население, и безопасное перемещение ресурсов, оборудования и персонала имеет важное значение. Удаленные и приватизированные операции могут испытывать трудности с поиском и сохранением ресурсов кибербезопасности.

Крупные компании и провайдеры изо всех сил пытаются управлять огромными кампусами, некоторые из которых эквивалентны небольшим городам, обслуживая миллионы пациентов каждый год и предоставляя работу десяткам тысяч человек. Обход систем управления зданием, коммунальными службами и системами безопасности может серьезно повлиять на уход за пациентами, а также на безопасность пациентов и медицинских работников. Учитывая, что национальный директор США по кибербезопасности определил приоритеты, те, кто первым применит методы целостной безопасности, должны наметить курс.

Путь вперед

Если устаревшие медицинские технологии, устройства IoMT и технологии объектов не являются предполагаемой целью киберинцидентов, каскадные воздействия могут сделать их бесполезными, что приведет к задержке лечения и потенциальному вреду как для пациентов, так и для поставщиков. Когда корпоративные ИТ-системы выходят из строя, они часто оказываются изолированными от остальной сети. Когда операционные системы выходят из строя, последствиями могут быть имущество и несчастные случаи.

Этот образ действий часто приводит к дихотомии между системами управления рисками и отчетами об инцидентах. В середине инциденты безопасности продолжают происходить. В связи с этим сценарием возникает вопрос: знают ли ИТ-специалисты и специалисты по инфраструктуре, что еще связано с сетями связи, и потенциальные возможности эксплуатации этих устаревших систем, устройств IoMT, сетей и систем управления?

Учитывая чрезмерную зависимость от технологий и бремя ручных операций, больницы и поставщики медицинских услуг снижают риски кибербезопасности, обеспечивая соответствие быстро меняющимся нормативным требованиям и работая над получением информации о подключении, трафике и аномалиях, связанных с их сетевым поведением.

При масштабе потенциальных рисков ключевую роль играет прозрачность. Решение по кибербезопасности, специально созданное для операционных технологий и Интернета вещей, может:

Захватитm и визуализировать ландшафт из десятков или сотен тысяч подключенных систем и конечных точек

Мониторить и проводить аудит сетевого трафика в режиме реального времени для охвата систем, не связанных с ИТ.

Понимать базовый и постоянный статус кибербезопасности организации

Предоставлять действенную информацию для решения наиболее важных проблем

Ограничить сторонний доступ и оповещение об изменениях поведения сети или переменных

Усилить политику безопасности организации без пробелов или теневого подключения». ***(Danielle Jablanski. Med-tech and health facilities: A cybersecurity house of mirrors // Breaking Media, Inc. (https://medcitynews.com/2022/09/med-tech-and-health-facilities-a-cybersecurity-house-of-mirrors/). 19.09.2022).***

***

Кіберзлочинність та кібертерроризм

«По словам Дженнифер Уильямс, директора по информационной безопасности пенсионного плана Healthcare of Ontario Pension Plan, фишинговые атаки и атаки программ-вымогателей являются одними из главных угроз для спонсоров пенсионных планов и институциональных инвесторов со стороны киберпреступников.

«Обычный подход киберпреступников начинается с простого фишингового электронного письма, предназначенного для того, чтобы сотрудник ошибочно отреагировал на запрос, что привело к компрометации информации его учетной записи пользователя. Это потенциально открывает дверь для инцидента с программами-вымогателями», — написала она в электронном письме Canadian Investment Review. «Финансовые организации являются особенно популярными объектами атак программ-вымогателей из-за высокой стоимости данных и затрат, связанных с нарушением операций».

В случаях программ-вымогателей организации-жертвы обычно блокируются в своих компьютерных системах с помощью программы шифрования данных. Учреждениям обычно остается выбирать между попытками вымогательства или раскрытием цифровой информации о третьих лицах.

«Эти типы атак могут иметь значительные финансовые последствия для организации и могут повлиять на уверенность их клиентов в их способности защитить свои системы и конфиденциальную информацию своих компаний», — отметила Уильямс.

Она также сказала, что риски, связанные с киберпреступностью для спонсоров пенсионных планов и их организаций, возросли с начала пандемии. «Поскольку эти атаки продолжают развиваться, организациям необходимо идти в ногу со временем

и опережать новые типы атак. Благодаря постоянному развитию технологий, использующих автоматизацию, машинное обучение и искусственный интеллект, киберпреступники также получают выгоду от использования аналогичных технологий для проведения более быстрых, эффективных и изощренных атак».

Чтобы ограничить риск, связанный с фишинговыми атаками и программами-вымогателями, она предложила спонсорам планов и другим институциональным инвесторам проявлять инициативу в своем подходе к безопасности. Для этого организации должны предоставить инвесторам четкое представление о существующих практиках и политиках безопасности.

«Инвесторы, напрямую или с помощью консультантов-специалистов, должны провести комплексную проверку, получив подробный обзор и понимание методов защиты данных организации, технологий, используемых для снижения рисков безопасности, мониторинга событий безопасности, процессов реагирования на инциденты и требований к обучению сотрудников».

Уильямс сказала, что надежные программы информационной безопасности обычно строятся на уровнях безопасности на технологическом, организационном и индивидуальном уровнях. Чтобы уменьшить угрозу, исходящую от киберпреступников, спонсоры пенсионных планов и институциональные инвесторы должны вкладывать средства в программы безопасности, которые обеспечивают организационный надзор и соответствуют передовым практикам и стандартам отрасли.

«Одних только технологий недостаточно. Важно потратить время на правильную настройку и оптимизацию этих технологий, чтобы добиться желаемого результата мониторинга аномалий в системной среде».

На институциональном уровне Уильямс предложила, чтобы организации регулярно проверяли осведомленность сотрудников о киберугрозах с помощью симуляции фишинговых атак. «Создание культуры, в которой осведомленность о безопасности имеет большое значение, [как есть] предлагая множество возможностей для обучения, чтобы помочь сотрудникам понять свою критическую роль в защите систем и конфиденциальной информации». ***(Gideon Scanlon. Phishing and ransomware risks on the rise for pension funds, says expert // Contex Group Inc. (https://www.benefitscanada.com/news/cir-news-news/phishing-and-ransomware-risks-on-the-rise-for-pension-funds-says-expert/). 02.09.2022).***

***

«Существуют десятки тысяч незаконных пиратских веб-сайтов, которые предлагают пользователям бесплатные фильмы, телепередачи и игры.

Это индустрия с оборотом около 2 миллиардов долларов.

Сама природа пиратских веб-сайтов означает, что они не регулируются, поскольку они уже являются незаконными, и новый отчет показал, что киберпреступники пользуются этим отсутствием регулирования.

В отчете Альянса цифровых граждан говорится, что 12% всей рекламы на пиратских веб-сайтах содержат вредоносное ПО.

«Следователи обнаружили на пиратских сайтах вредоносное ПО, предназначенное для получения доступа к устройству пользователя с целью кражи

банковской информации, загрузки шпионского ПО для отслеживания действий пользователя или отметки его для потенциальной атаки в будущем», — говорится в отчете.

Киберпреступники могут наживаться на пользователях всего за несколько кликов.

«Преступники используют очень хитрую, но опасную схему кликов», — сказал Том Гэлвин, исполнительный директор Альянса цифровых граждан.

Иногда это может выглядеть как реклама, предлагающая бесплатный продукт, или это может быть тактика запугивания, чтобы убедить пользователей передать информацию.

Галвин сказал, что собственные следователи его организации подверглись атаке программы-вымогателя, когда изучали проблему на пиратском веб-сайте.

«Наш компьютер был захвачен, — сказал Гэлвин. «Наши файлы были зашифрованы, а затем мы получили сообщение с требованием денег, чтобы иметь возможность расшифровать эти файлы и снова получить к ним доступ».

Отчет показал, что почти 8 из 10 исследованных пиратских сайтов содержали рекламу с вредоносным ПО.

«Мы находимся на пороге эпидемии вредоносного ПО, и простой поиск на пиратских веб-сайтах бесплатных фильмов, телешоу и игр способствует этому», — сказал Гэлвин.

Этот отчет появился в связи с тем, что правоохранительные органы и члены Конгресса расследуют общий рост атак программ-вымогателей в последние годы.

Ранее в этом году Министерство внутренней безопасности свидетельствовало об опасности для всех.

«Они нацелены на крупные и более мелкие цели, будь то крупные корпорации, малые или средние предприятия, больницы, местные органы власти или школы», — сказал Иранга Кахангама, помощник секретаря по кибербезопасности, инфраструктуре, рискам и устойчивости Управления стратегии, политики и планов. Министерство внутренней безопасности США во время слушаний в Палате представителей в июне.

Галвин надеется, что новые данные заставят пользователей дважды подумать, прежде чем заходить на пиратский сайт.

«Когда кто-то заходит на пиратский веб-сайт и заражается, это может привести к закрытию малого бизнеса», — сказал Галвин. «Это может привести к компрометации серьезных конфиденциальных документов».

Галвин сказал, что группа взаимодействует с государственными организациями и рекламным сообществом для решения этой проблемы, а также создает образовательные программы для пользователей об опасностях». ***(Samantha Manning. Report finds 12% of ads on piracy websites involve malware to target users // Cox Media Group (https://www.wpxi.com/news/local/report-finds-12-ads-piracy-websites-involve-malware-target-users/H5WZ75KY6BDPPB7FUQOWFW6L4Q/). 14.09.2022).***

***

«…По данным исследовательской компании Cybersecurity Ventures, глобальные издержки от киберпреступлений ежегодно растут на 15% и, по прогнозам, к 2025 году достигнут 10,5 трлн долларов. Если бы ее измеряли как страну, киберпреступность была бы третьей по величине экономикой в мире после США и Китая.

Атаки программ-вымогателей, предназначенных для нанесения вреда организациям путем блокировки их компьютерных систем до тех пор, пока они не заплатят криптовалютой, особенно популярны. Агентство кибербезопасности и безопасности инфраструктуры (CISA) сообщило, что в прошлом году 14 из 16 секторов критической инфраструктуры страны подверглись атакам программ-вымогателей.

Поскольку все стало цифровым, компании и правительственные учреждения должны столкнуться с тревожной реальностью: достаточно одного человека в организации, чтобы у него был плохой день — будь то Боб из финансового отдела, которого фишинговое электронное письмо обманом заставило нажать на вредоносное ПО или Бетси из ИТ-отдела, которая толстыми пальцами нажимает на команду при настройке сетевого устройства — подвергать свои предприятия хакерам. В киберзащите вы всегда являетесь самым слабым звеном в своей цепи.

Заманчиво полагать, что одна только технология может решить всю проблему кибербезопасности, но, хотя решения для защиты и восстановления после атак эффективны и бесценны, они являются лишь частью головоломки.

Для победы в войне, в которой злоумышленники постоянно придумывают новые уловки, необходим больший поток данных об угрозах и сообщений о нарушениях безопасности посредством формальных процессов. Нам нужны лидеры и коллеги по кибербезопасности как в государственном, так и в частном секторах, чтобы не отставать от плохих парней, постоянно сотрудничая, координируя и поддерживая связь друг с другом.

В конце концов, бизнес и правительство тесно взаимосвязаны в попытках решить проблему кибербезопасности. Чтобы доказать это, достаточно взглянуть на взлом SolarWinds, в ходе которого злоумышленники, предположительно действовавшие под руководством российской разведки, получили конфиденциальную правительственную информацию, нацелившись на компании с государственными контрактами.

Если корпоративные и государственные эксперты по безопасности не станут более целенаправленно и систематически узнавать друг у друга в реальном или почти реальном времени о последних угрозах, критически важная информация будет слишком часто оставаться разрозненной. Мир больше не может себе этого позволить. Киберзащита должна быть командной.

К счастью, есть признаки прогресса. В середине марта президент Байден подписал Закон об усилении американской кибербезопасности, который требует от предприятий, считающихся «критической инфраструктурой», сообщать об инцидентах кибербезопасности в федеральное агентство в течение 72 часов, а о любых платежах программ-вымогателей — в течение 24 часов.

Несмотря на то, что CISA все еще разрабатывает детали реализации, закон расширит коллективные знания страны о кибератаках, создав запись для всеобщего

обозрения об использованных уязвимостях, средствах защиты, типах скомпрометированной информации и, если известна любая информация о нападавших.

Кроме того, Указ президента Байдена об улучшении национальной кибербезопасности, изданный в мае 2021 года, включает действия, направленные на устранение барьеров для обмена информацией об угрозах между государственным и частным секторами.

Приказ предписывал CISA работать с Управлением по вопросам управления и бюджета, чтобы рекомендовать формулировки контракта, которые упрощают обмен критически важными данными, и учредил Наблюдательный совет по кибербезопасности под совместным председательством представителей государственного и частного секторов, чтобы собраться после крупного кибер-инцидента, проанализировать что произошло, и дать рекомендации по улучшению безопасности.

Эти меры являются полезным началом, но любой, кто перешел из государственного сектора в частный, как я сделал в мае, когда я оставил свою должность исполняющего обязанности директора по информационной безопасности (CISO) в ЦРУ на аналогичную должность в компании по кибербезопасности Rubrik. — хорошо осознает потребность в более существенном партнерстве по обмену разведданными об угрозах.

Но как? Вот несколько идей:

1. Директора по информационной безопасности часто неформально обсуждают друг с другом происходящее, но их идеи остаются внутри группы. Это упускает возможность информировать других и приводит к изоляции срочных знаний. Должен быть способ распространять информацию об угрозах и лучшие практики для более широкой аудитории.

Например, в июне моя компания поручила Крису Кребсу, первому директору CISA, создать и возглавить стратегический консультативный совет по вопросам информационной безопасности, чтобы помочь организациям частного и государственного секторов справиться с распространением программ-вымогателей и других кибератак. Это пример того, насколько ценным может быть участие компаний из индустрии кибербезопасности вместе с ключевыми заинтересованными сторонами в правительстве в качестве центров обмена информацией и обращений к властям в отношении последних угроз и способов их смягчения.

2. Компания может спонсировать сеть лидеров и органов власти в области кибербезопасности, аналогичную сети Peer Connect от Gartner, которая описывает себя как «самую влиятельную в мире сеть бизнес-лидеров» и «сообщество ваших коллег для обсуждения ключевых вопросов и информирования ваших критических деловые решения».

3. Любой желающий может посетить веб-сайт Государственного департамента и узнать об угрозах в любой стране, от вооруженных столкновений до преступности и болезней, прежде чем принять решение о поездке туда. Министерство внутренней безопасности поддерживает Национальную консультативную систему по борьбе с терроризмом, которая предоставляет своевременную и подробную информацию о

террористических угрозах. Возможно, CISA может сделать что-то подобное в области кибербезопасности.

Наличие таких открытых каналов связи значительно улучшило бы состояние кибербезопасности страны. Нам нужно, чтобы те, кто находится на передовой, постоянно учились друг у друга. При более тесном сотрудничестве киберпреступники столкнутся с защитой, которая больше, чем сумма ее частей». ***(Michael Mestrovich. Technology alone can't solve the cybersecurity problem; we need better information sharing // NEXSTAR INC. (https://thehill.com/opinion/cybersecurity/3624552-technology-alone-cant-solve-the-cybersecurity-problem-we-need-better-information-sharing/). 01.09.2022).***

***

«Развивающийся цифровой ландшафт в Северной и Южной Америке усугубил проблемы и уязвимости в отношении кибербезопасности. В настоящее время страны региона сталкиваются с атаками киберпреступников, начиная от компрометации корпоративной электронной почты и онлайн-мошенничества и заканчивая программами-вымогателями и отмыванием денег.

Финансово мотивированные группы не только атаковали организации по всей Латинской Америке, в первую очередь с помощью программ-вымогателей, но и расширили сферу своей деятельности. Например, в первой половине 2020 года в Латинской Америке были зарегистрированы самые высокие в мире показатели кибератак: почти в три раза больше атак через мобильные браузеры, чем в среднем по миру.

Например, Коста-Рика стала жертвой крупномасштабных атак программ-вымогателей, инициированных группой под названием Conti в апреле 2022 года. Кибератака, начавшаяся в министерстве финансов Коста-Рики, в конечном итоге затронула 27 различных министерств в серии взаимосвязанных атак. Действия Конти привели к тому, что части цифровой инфраструктуры Коста-Рики были парализованы на несколько месяцев, в то же время нарушив систему общественного здравоохранения и заработную плату некоторых работников государственного сектора.

Telecom Argentina, один из крупнейших интернет-провайдеров Аргентины, также подверглась крупной атаке программы-вымогателя, в которой участвовало около 18 000 компьютеров в 2020 году. В этом инциденте хакеры потребовали выкуп в размере 7,5 миллионов долларов, а сотрудникам был запрещен доступ к базам данных и внутренним VPN.

В этом контексте 12-16 сентября в Буэнос-Айресе, Аргентина, состоялось 7-е совещание американской рабочей группы Интерпола по киберпреступности для оценки угроз и тенденций в регионе. Встреча собрала более 90 участников из 32 стран-членов, 4 международных организаций и 13 государственных и частных организаций.

Среди ключевых приоритетов Группа обсудила Глобальную стратегию борьбы с киберпреступностью на 2022–2025 годы, которая будет опубликована в конце этого года. Эта стратегия будет способствовать углубленному пониманию

угрозы киберпреступности и расширению возможностей по предотвращению, обнаружению, расследованию и пресечению кибератак.

Группа также обсудила создание американского отдела для координации операций по борьбе с киберпреступностью. Это согласуется с глобальной стратегией Интерпола, при этом другие отделы ранее были созданы в Африке и регионах АСЕАН.

Другие темы были посвящены инициативам по реагированию на киберпространство, расследованию криптовалют, новым киберугрозам в Северной и Южной Америке и обмену следственной информацией.

«Эта рабочая группа — хорошая возможность укрепить сотрудничество полиции на международном и региональном уровнях, чтобы мы могли более эффективно бороться с киберпреступностью и сделать мир более безопасным», — сказал Хуан Карлос Эрнандес, начальник федеральной полиции Аргентины.

Киберпреступникам открылся путь к новым технологиям, поскольку они атакуют с большей частотой и эффективностью. Недостаточное внимание к безопасности, а также компьютерные уязвимости предоставляют киберпреступникам возможности для незаконной выгоды с низким уровнем риска и высокой прибылью.

Столкнувшись с этой растущей угрозой, Интерпол провел ряд мероприятий в Латинской Америке, чтобы повысить осведомленность о киберпреступности и способствовать более тесному региональному сотрудничеству. Ключевые мероприятия включали учебные курсы по полицейским возможностям Интерпола, цифровой криминалистике, разведке с открытым исходным кодом, криптовалютам и расследованиям темной сети.

Такая деятельность подпадает под действие Проекта Cyber Americas (финансируется Министерством внутренних дел Канады) и Расширенного проекта глобальных действий по борьбе с киберпреступностью (GLACY+), совместной инициативы Европейского Союза и Совета Европы». ***(INTERPOL Working Group Highlights Cyber Threats Across the Americas // Homeland Security Today (https://www.hstoday.us/subject-matter-areas/cybersecurity/interpol-working-group-highlights-cyber-threats-across-the-americas/). 20.09.2022).***

***

«Федеральное бюро расследований (ФБР) предупредило о широко распространенном использовании прокси-серверов и конфигураций для маскировки и автоматизации атак с заполнением учетных данных. ФБР предупредило, что злоумышленники широко использовали резидентные прокси-серверы вместо тех, которые подключены к центрам обработки данных, чтобы избежать срабатывания мониторов подозрительного поведения.

«Атаки с заполнением учетных данных, обычно называемые взломом учетных записей, применяют действительные комбинации имени пользователя и пароля, также известные как учетные данные пользователя или «комбинированные списки», из ранее скомпрометированных онлайн-ресурсов или утечек данных», — пояснили в ФБР.

Центр интернет-преступности ФБР (IC3) при содействии Федеральной полиции Австралии выпустил Уведомление для частных компаний, чтобы предупредить потенциальных жертв атак с подменой учетных данных.

По данным агентства, атаки в основном были направлены на медиа-компании, розничную торговлю, здравоохранение, рестораны и компании по доставке еды. Их влияние включает финансовые потери от мошеннических покупок, простоев системы, уведомлений клиентов и репутационного ущерба.

Действительные учетные данные от атак с заполнением учетных данных в продаже на общедоступных веб-сайтах.

ФБР наблюдало за двумя общедоступными веб-сайтами с более чем 175 000 зарегистрированных клиентов. Поверхностные веб-сайты продавали более 300 000 уникальных наборов учетных данных, украденных с помощью атак с заполнением учетных данных, с транзакциями на сумму более 400 000 долларов.

Кроме того, киберпреступники продавали хакерские конфигурации, нацеленные на определенные веб-сайты, и инструменты для взлома паролей другим злоумышленникам в даркнете.

Конфиги содержали адрес целевого веб-сайта, как сформировать HTTP-запрос, определить успешные или неудачные попытки и нужны ли прокси для входа.

Точно так же они предоставили видеоуроки в темной сети и социальных сетях, обучая других, как взламывать учетные записи с помощью атак с заполнением учетных данных и других методов.

«Злоумышленники выходят на новый уровень изощренности, намного превышающий тот, с которым могут справиться только пароли и даже MFA, — сказал Гуннар Петерсон, директор по информационным технологиям в Forter. «Это связано с тем, что атаки нацелены на уровни контроля доступа и идентификации, чтобы обойти защиту, которая окружает данные и учетные записи компании».

Мобильные приложения более уязвимы для атак с заполнением учетных данных.

ФБР предупредило, что злоумышленники нацелены как на веб-сайты, так и на мобильные приложения. Однако мобильные приложения легче взломать, потому что они имеют более слабые протоколы безопасности.

Кроме того, мобильные приложения допускали больше попыток входа в систему, увеличивая количество проверок в минуту (CPM), что гарантировало более быструю проверку украденных учетных данных для входа.

ФБР заметило, что злоумышленники часто использовали Burp Suite, Fiddler и Wireshark для понимания механизма аутентификации веб-сайтов и мобильных приложений.

Хакеры используют резидентные прокси для обхода защиты веб-сайтов

ФБР сообщает, что злоумышленники используют прокси-серверы и конфигурации для атак на мобильные приложения или веб-сайты компаний.

Злоумышленники приобрели резидентные прокси-серверы, чтобы скрыть IP-адрес, который веб-сайты будут блокировать из-за происхождения из определенных географических регионов.

В предупреждении говорилось, что злоумышленники предпочитают резидентные прокси, потому что они генерируют меньше подозрительной

активности, чем прокси, подключенные к центрам обработки данных. Таким образом, протоколы безопасности редко блокируют или помечают резидентные прокси-серверы по сравнению с их аналогами в центрах обработки данных.

«Выполняя успешные атаки с заполнением учетных данных, киберпреступники в значительной степени полагались на использование резидентных прокси-серверов, которые подключены к резидентным интернет-соединениям и, следовательно, с меньшей вероятностью будут идентифицированы как ненормальные», — отмечает агентство.

Хакеры обычно получают резидентные прокси, взламывая уязвимые сетевые устройства, такие как маршрутизаторы и устройства IoT, без ведома владельцев.

Рекомендации ФБР по атакам с подменой учетных данных

ФБР рекомендовало включить многофакторную аутентификацию (MFA) в качестве дополнительного уровня для защиты от атак с подменой учетных данных, особенно из необычных или неожиданных стран.

Агентство также призвало онлайн-сервисы применять методы снятия цифровых отпечатков пальцев, чтобы обнаруживать, когда один пользователь или IP-адрес пытается войти в систему с нескольких учетных записей.

Веб-сайты и мобильные приложения также должны применять теневой бан, который ограничивает доступ пользователей к учетной записи без явных признаков. Теневой запрет не позволяет злоумышленнику определить легитимность украденных действительных учетных данных.

Кроме того, операторы веб-сайтов и мобильных приложений должны отслеживать строки пользовательского агента, используемые в инструментах заполнения учетных данных, и блокировать их.

Организации также должны искать конфигурации взлома учетных записей, адаптированные для их веб-сайтов, и изменять конфигурации целевого веб-сайта, чтобы сделать конфигурации неэффективными.

Наконец, операторы веб-сайтов не должны полагаться исключительно на CAPTCHA для предотвращения атак с заполнением учетных данных, поскольку злоумышленники могут легко решать CAPTCHA с помощью автоматизированных инструментов.

«Когда злоумышленник может использовать пароль, сброс профиля учетной записи или приглашение MFA в злонамеренных целях, защитный слой компании отпадает», — добавил Петерсон. «Это означает, что такие технологии, как снятие отпечатков пальцев и мониторинг захвата учетных записей, важнее, чем когда-либо».

По словам Ральфа Пизани, президента Exabeam, индустрия кибербезопасности должна переосмыслить использование паролей для предотвращения атак, прежде чем они увенчаются успехом.

«Учетные данные должны быть главными воротами замка — они представляют собой новый периметр, но SOC по-прежнему не могут обнаруживать атаки на основе учетных данных», — сказал Пизани.

Он рекомендовал «надлежащее обучение, циклы обратной связи, наглядность и эффективные технические возможности» для устранения утечки учетных данных.

«Недавнее уведомление ФБР США о конфиденциальности — яркое напоминание о том, что организациям и пользователям их веб-сайтов еще многое предстоит узнать об эффективной безопасности паролей», — сказал Нил Джонс, директор по пропаганде кибербезопасности Egnyte.

«К сожалению, слабые пароли могут стать буквально игровой площадкой для кибер-злоумышленников, особенно когда они получают доступ к решению удаленного доступа вашей организации для просмотра идентификационных данных корпоративных пользователей или к системам электронной почты, чтобы выдавать себя за ваших законных сотрудников». ***(Alicia Hope. FBI Alert: Hackers Leverage Residential Proxies and Custom Configs To Execute Credential Stuffing Attacks // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/fbi-alert-hackers-leverage-residential-proxies-and-custom-configs-to-execute-credential-stuffing-attacks/). 05.09.2022).***

***

«…DDoS-атаки остаются серьезной проблемой. Предприятия, основанные на информационных технологиях, небольшие компании и мегакорпорации — все они являются потенциальными целями таких кибератак, которые могут привести к полной остановке операций.

Что такое DDoS-атака?

Это тип кибератаки, направленной на переполнение сервера вредоносным трафиком, что приводит к временному или постоянному закрытию веб-сайта.

Обычно он выполняется с использованием зараженных вредоносным ПО устройств, называемых ботами, а их кластер называется ботнетом. Эти боты включают ноутбуки, смартфоны, смарт-телевизоры, носимые устройства, термометры, камеры видеонаблюдения, автомобильные информационно-развлекательные системы и т. д.

Итак, на какие отрасли нацелены DDoS-атаки? Обычно они нацелены на игры, программное обеспечение и технологии, средства массовой информации и развлечения, финансы, интернет и телекоммуникации.

Некоторые популярные инструменты, используемые во время DDoS-атаки, включают LOIC, HULK, Tor's Hammer, RUDY, DDoSISM, Slowloris, Golden Eye и HOK.

Раннее и точное обнаружение имеет ключевое значение

Раннее обнаружение и мониторинг трафика имеют решающее значение для предотвращения DDoS-атак. Вы можете управлять, отслеживать и фильтровать вредоносный трафик, запросы и пакеты данных с помощью программ интеллектуального сканирования и брандмауэров.

Брандмауэр — это элемент сетевой безопасности, используемый для уточнения входящего и исходящего сетевого трафика в соответствии с выбранными стандартами безопасности и протоколами.

Это поможет вам автоматически или вручную различать нормальные и опасные запросы на основе поведения, шаблонов и анализа сигнатур. Более того, эти интеллектуальные инструменты помогают блокировать вредоносные запросы, предотвращая DDoS-атаки.

В наши дни брандмауэры работают на основе искусственного интеллекта, чтобы в первую очередь сканировать уязвимости и устранять их. Однако методы обнаружения DDoS-атак выходят далеко за рамки одних только брандмауэров.

Индикаторы DDoS-атак

Чтобы знать, как идентифицировать DDoS-атаку, вы должны знать следующие индикаторы. Вы можете использовать эти сигналы для автоматизации инструментов обнаружения DDoS-атак для своевременных уведомлений.

Слишком много неожиданных запросов для определенного IP-адреса

Этот индикатор можно использовать, чтобы временно дать вашему маршрутизатору команду отправлять трафик на маршруты blackhole с определенного IP-адреса. Черная дыра — это сетевое пятно, где отбрасывается входящий или исходящий трафик.

Направление маршрутизатора просто заведет атакующий IP-адрес в тупик, тем самым защитив ваши серверы. Однако делать это не рекомендуется, так как вы также заблокируете любой невредоносный трафик.

С помощью этого индикатора вы не можете настроить оповещения о программах предотвращения и обнаружения DDoS-атак, поскольку они также будут выделять легитимных ботов.

Итак, как вы можете остановить различные типы DDoS-атак, обнаружив необычный трафик? Ответ прост: вы можете настроить оповещения, когда определенный IP-адрес отправляет слишком много запросов за короткое время. Это лучше всего работает с методом внесения в белый список, так как будут исключения, такие как Googlebots.

Сервер отображает «Ошибка 503»

Ошибка HTTP 503 указывает на то, что сервер веб-сайта недоступен или не может обрабатывать какие-либо запросы, что может быть связано с DDoS-атакой.

Вы можете настроить оповещения всякий раз, когда происходит определенное событие. В Windows это можно сделать в средстве просмотра событий. Прикрепите задачу к любому событию, которое считается заслуживающим расследования, например «Ошибка 503».

Задачу можно прикрепить в два простых шага:

Откройте средство просмотра событий и щелкните правой кнопкой мыши событие.

Откроется экран конфигурации. Заполните столбцы, чтобы отправить уведомления по электронной почте выбранному персоналу.

Тайм-аут TTL

TTL — это сокращение от Time to Live — время, в течение которого пакет существует в сети до того, как маршрутизатор отвергнет его. Вы можете автоматизировать пинг-оповещения, и некоторые поставщики услуг делают это. Таким образом, ваш сайт будет контролироваться круглосуточно. Время пинга — это время, необходимое для передачи небольших наборов данных с устройства на сервер.

Это работает по тому принципу, что DDoS-атаки или DoS-атаки потребляют чрезмерную пропускную способность; поэтому время пинга будет слишком длинным или истечет время вообще.

Встроенный и внеполосный мониторинг

Проверка пакетов на линии и внеполосный мониторинг — это методы обнаружения DDoS-атак как для облака, так и для локальной среды.

Как только вы узнаете, как работает DDoS-атака, вы можете использовать инструменты, размещенные на основном пути данных, называемые встроенными, или установленные вне пути, называемые внеполосными. Давайте узнаем больше об этих методах обнаружения

Встроенная защита от DDoS-атак

Встроенные инструменты защиты от DDoS-атак работают в центре обработки данных или в качестве уровня предотвращения и обнаружения DDoS-атак, установленного над вашей инфраструктурой.

Такие инструменты отслеживают как затронутый, так и не затронутый трафик, где вредоносные запросы фильтруются, разрешая входящий и исходящий только законный трафик.

Инструменты изучают нормальные модели трафика, тем самым обнаруживая аномальные действия.

Преимущества встроенных средств защиты от DDoS-атак

Быстро обнаруживает вредоносный трафик, нейтрализуя атаку.

Никаких неопределенных сетевых сбоев.

Использует механизмы обучения для самостоятельной настройки конфигураций защиты.

Знает, как определить DDoS-атаку, не основанную на томах.

Никакого дополнительного оборудования, такого как анализаторы потока и инструменты BGP, не требуется.

Этот метод обнаружения DDoS-атак может использовать настоящие службы безопасности уровня 7.

Недостатки встроенной защиты от DDoS-атак

Высокая вероятность ложных срабатываний при ненормальном использовании IP.

Увеличенная задержка.

Внеполосная защита от DDoS-атак

Внеполосные инструменты пассивно обрабатывают пакетные данные для оценки определенных аспектов потоков данных в реальном времени. IDS или система обнаружения вторжений — это инструмент внешней защиты, используемый для мониторинга и фильтрации трафика.

Преимущества внешней защиты от DDoS-атак

Может использоваться для обнаружения и предотвращения атак на основе объема.

Нет увеличенной задержки в режиме без атаки, так как трафик не проверяется.

Низкая вероятность ложных срабатываний.

Недостатки внешней защиты от DDoS-атак

Медленное обнаружение.

Смягчение требует времени из-за неопределенных сетевых сбоев.

Не удается автоматически настроить конфигурацию защиты.

Медленные службы безопасности уровня 7 невозможны.

Требуется дополнительное оборудование, такое как анализаторы и инструменты BGP.

Дополнительные советы

По сравнению с 2020 годом, в 2021 году число DDoS-атак выросло на 11% и достигло почти 5,4 миллиона. Такие данные делают еще более важным понимание мотивов DDoS-атак и способов их своевременного обнаружения.

Вот еще несколько полезных советов о том, как определить DDoS-атаку.

Веб-сканеры, WAF и обнаружение аномалий трафика

Веб-сканеры, брандмауэр веб-приложений (WAF) и средства обнаружения аномалий трафика DDoS-атак могут помочь уменьшить ущерб и профилировать трафик. Веб-сканеры регулярно отслеживают веб-приложения, особенно после атаки, а WAF фильтрует трафик с помощью алгоритмов машинного обучения.

Они работают, замечая необычные действия, выявляя и блокируя ботов и отправляя данные в центр очистки для анализа и дальнейших действий.

Встройте обнаружение DDoS в свою инфраструктуру

Ваша ИТ-структура должна быть защищена надежной защитой, предотвращающей объемные и протокольные DDoS-атаки. Никогда не игнорируйте никакие обновления программного обеспечения, так как они могут содержать код, способный противостоять новым методам, используемым злоумышленниками.

Инфраструктура, устойчивая к DDoS, управляет избыточным трафиком при атаке на сервер. Такие решения могут направлять трафик в центры очистки для проверки сетевых запросов, фильтрации законного трафика и применения правил и политик для смягчения будущих атак.

Резюме

DDoS-атаки перегружают серверы вредоносным трафиком, что приводит к временному или постоянному закрытию веб-сайта. Компании могут предотвращать и обнаруживать такие угрозы, используя встроенные или внешние средства защиты.

Вы также можете настроить оповещения о слишком большом количестве неожиданных запросов с определенного сервера. В этом случае они могут начать фильтровать вредоносные запросы с помощью инструментов.

Веб-сканеры и брандмауэры могут помочь смягчить последствия атаки или даже предотвратить ее. Они могут наблюдать необычные действия, связанные с сетью, а также генерировать предупреждения.

Устойчивая к DDoS-атакам инфраструктура вместе с правильными инструментами обнаружения DDoS-атак могут эффективно сдерживать такие атаки. ***(Knarik Petrosyan. How to Detect DDoS Attacks? // Techstrong Group Inc. (https://securityboulevard.com/2022/09/how-to-detect-ddos-attacks/). 09.09.2022).***

***

«Киберпреступность растет, и оказывается, что мета-приложения особенно ей подвержены. TechShielder недавно провел исследование, которое показало, что Facebook, Instagram и WhatsApp являются одними из самых уязвимых приложений для различных кибератак. Это исследование было проведено путем анализа ежемесячного объема поиска, и эти три приложения вошли

в тройку лидеров в поисковом рейтинге, при этом все было учтено и принято во внимание.

После всего сказанного, важно отметить, что объем поиска по ключевым словам «Facebook взломан» колебался на уровне около 550 000. Следующим в отдаленной секунде был Instagram с чуть менее 250 000, или 246 000, если быть точным. WhatsApp показал себя лишь немногим лучше: слова «WhatsApp взломан» были найдены около 135 000 раз.

Что еще более тревожно, так это то, что даже наименее уязвимое приложение Meta почти в три раза превышало объем поиска, чем Snapchat, который занял четвертое место с 49 500. На пятом месте оказалось приложение для прямых трансляций Twitch, набравшее всего 27 100 человек, так что это явно проблема, которая затрагивает Meta непропорционально больше, чем любая другая крупная платформа.

Иными словами, средний пользователь Facebook примерно в 10 раз чаще подвергается взлому, чем средний пользователь Snapchat. Несмотря на то, что это так, Facebook имеет гораздо большее количество пользователей, что, очевидно, увеличивает количество взломанных аккаунтов.

Это исследование выявило риски, связанные с обменом данными с третьими лицами для кибербезопасности, поскольку такие действия потенциально могут привести к тому, что злоумышленники получат больше источников данных для взлома. У Facebook самое большое количество точек доступа из всех, поэтому у него в десять раз больше взломанных аккаунтов, несмотря на то, что у него в четыре-пять раз больше пользователей, чем у Snapchat. Это говорит о том, что пользователь Facebook как минимум в два раза чаще подвергается взлому, чем пользователь Snapchat.

Еще одна вещь, на которую это исследование пролило свет, — это частота кибератак по городам. Лондон оказался очагом кибератак, получив 4260 баллов. Это означает, что у пользователей гораздо больше шансов быть взломанными, если они живут в Лондоне, чем в противном случае.

На втором месте оказался Мехико, хотя его результат в 2540 баллов был намного меньше, чем у Лондона. В Лондоне явно существует очень серьезная проблема с киберпреступностью, и, если не будут предприняты необходимые шаги, маловероятно, что эта проблема исчезнет в ближайшее время.

Париж был третьим худшим местом для киберпреступности с оценкой 2 190, сопровождаемой Боготой с оценкой 2 060. Интересно, что ни один город, кроме Лондона, не превысил 3000, не говоря уже о 4000, что просто показывает, что проблема киберпреступности в Лондоне достигает непредвиденных высот.

Нам придется подождать и посмотреть, будет ли что-нибудь сделано для борьбы с ростом киберпреступности во всем мире. Такие компании, как Meta, усугубляют ситуацию из-за своей спекуляции, и не похоже, что они изменят свои методы в ближайшее время. Скорее, они удваивают обмен данными с третьими сторонами, что увеличивает объем кибератак». ***(Zia Muhammad. This Research Shows Meta Apps Are Extremely Vulnerable to Cyber Attacks // Digital Information World (https://www.digitalinformationworld.com/2022/09/this-research-shows-meta-apps-are.html). 20.09.2022).***

***

«Известно, что наряду с документально подтвержденными финансовыми потерями и ущербом для репутации, кибератаки в сфере здравоохранения ставят под угрозу безопасность пациентов и отрицательно сказываются на оказании медицинской помощи.

Чтобы понять, как различные типы кибератак в сфере здравоохранения могут повлиять на безопасность пациентов, Proofpoint поручила Ponemon Institute провести опрос специалистов в области ИТ и ИТ-безопасности в секторе здравоохранения. В опрос были включены ответы 641 эксперта в данной области.

ПОСЛЕДСТВИЯ ДЛЯ БЕЗОПАСНОСТИ ПАЦИЕНТОВ

В частности, исследователи сосредоточились на четырех распространенных типах кибератак в сфере здравоохранения: программы-вымогатели, компрометация деловой электронной почты (BEC), компрометация облачных вычислений и атаки на цепочку поставок. Почти 90 процентов всех респондентов заявили, что их организации подверглись хотя бы одной кибератаке за последние 12 месяцев.

Хотя взаимосвязь и причинно-следственную связь трудно определить с абсолютной уверенностью, результаты показали, что респонденты опроса, имеющие повседневный опыт работы в этой области, ощутили ощутимое воздействие кибератаки на уход за пациентами с угрожающей скоростью.

Например, на вопрос, как атака программы-вымогателя повлияла на безопасность пациентов и оказание медицинской помощи в их организациях, 64 процента респондентов сообщили о задержках в процедурах и тестах.

Кроме того, 24 процента респондентов сообщили об увеличении уровня смертности, а 59 процентов заявили, что это привело к более длительному пребыванию. Половина респондентов заявили, что увеличилось количество пациентов, переведенных в другие учреждения.

В целом атаки программ-вымогателей оказали наибольшее влияние на безопасность пациентов в глазах ИТ-специалистов и специалистов по ИТ-безопасности. Более 70 процентов респондентов сообщили, что считают, что их организации уязвимы для программ-вымогателей.

Неудивительно, что программы-вымогатели были главной проблемой для киберлидеров, но организации сообщали о еще более высоком уровне уязвимости к компрометации облака (75 процентов). За последние два года 54% респондентов заявили, что их организация сталкивалась как минимум с одним взломом облака. Те, кто столкнулся с облачной компрометацией, сообщили о высокой частоте задержек в процедурах и тестах, а 18 процентов респондентов сообщили о росте смертности.

В отчете также отмечается распространенность атак компрометации деловой электронной почты (BEC), которые включают социальную инженерию, фишинг и спуфинг. Чуть более половины респондентов заявили, что они столкнулись как минимум с одним случаем BEC за последние два года, а 64 процента респондентов сообщили, что считают, что их организации уязвимы для атак BEC.

Помимо программ-вымогателей, BEC-атаки оказали наиболее значительное влияние на безопасность пациентов во многих категориях. Шестьдесят процентов респондентов сообщили о задержках в процедурах, а 48 процентов сообщили о более

длительном пребывании. Кроме того, 51 процент респондентов сообщили об увеличении осложнений от медицинских процедур.

Последней категорией, проанализированной исследователями, были атаки на цепочки поставок, из которых 71% организаций считали себя уязвимыми. Половина респондентов заявили, что за последние два года их организации подверглись как минимум одной атаке на цепочку поставок. Атаки на цепочку поставок оказали такое же влияние на уровень смертности, как и атаки программ-вымогателей: 21% респондентов сообщили о повышении уровня смертности после атаки на цепочку поставок.

Кроме того, 48 процентов респондентов сообщили об увеличении осложнений от медицинских процедур, а 51 процент сообщили о более длительном пребывании.

Результаты опроса показали значительную связь между кибератаками на здравоохранение и сбоями в повседневной работе, которые могут негативно сказаться на безопасности пациентов. Эти результаты еще раз подчеркивают необходимость уделения приоритетного внимания кибербезопасности в здравоохранении.

ОТСУТСТВИЕ ГОТОВНОСТИ, КАДРОВЫЕ ПРОБЛЕМЫ ДЕЛАЮТ ЗДРАВООХРАНЕНИЕ УЯЗВИМЫМ

Судя по данным, несмотря на выраженную серьезную обеспокоенность по поводу различных направлений атак и уязвимостей, эксперты по кибербезопасности в сфере здравоохранения все еще пытаются получить ресурсы, необходимые для того, чтобы действительно расставить приоритеты в области кибербезопасности.

Более половины респондентов указали на нехватку собственных специалистов как на главную проблему для эффективного обеспечения кибербезопасности, а половина респондентов отметили отсутствие сотрудничества с другими подразделениями.

Почти половина респондентов заявили, что в их организациях не хватает кадров, а 41 процент респондентов указали на бюджет как на узкое место. Более того, 40 процентов респондентов заявили, что кибербезопасность не считается приоритетом в их организациях, а 35 процентов заявили, что их организации не понимают, как защититься от кибератак.

В то время как 64 процента респондентов назвали небезопасные медицинские устройства своей главной проблемой кибербезопасности, только 51 процент заявили, что в их организациях действуют политики и процедуры для предотвращения атак на эти устройства и реагирования на них.

Кроме того, менее половины респондентов заявили, что предприняли шаги для предотвращения атаки BEC. Вместо этого организации больше внимания уделяют защите своих облачных сред и подготовке к атакам программ-вымогателей.

ЭФФЕКТИВНОЕ СНИЖЕНИЕ КИБЕРРИСКА

Несмотря на эти недостатки, многие организации здравоохранения по-прежнему предпринимают активные шаги по усилению своих мер безопасности. Сочетание различных стратегий обнаружения, предотвращения и реагирования может помочь организациям значительно снизить риск.

Почти 60 процентов респондентов заявили, что их организации предприняли шаги для информирования сотрудников о киберугрозах, а 63 процента заявили, что

они проводят регулярные программы обучения и повышения осведомленности. Программы обучения сотрудников имеют решающее значение для снижения риска внутренних угроз и обеспечения того, чтобы сотрудники распознавали признаки фишинга и других методов социальной инженерии.

Шифрование, токенизация и другие криптографические инструменты были популярны среди респондентов, когда речь шла о защите конфиденциальной информации в облаке. Кроме того, большинство респондентов заявили, что пользуются услугами безопасности премиум-класса, предоставляемыми их поставщиком облачных услуг.

«Обеспечение безопасности без снижения производительности пользователей считается важным элементом стратегии кибербезопасности организаций», — говорится в отчете.

«Для организаций здравоохранения крайне важно иметь продуктивную рабочую силу, эффективно защищая конфиденциальную информацию о пациентах. Потеря производительности также является самой большой статьей расходов при реагировании на кибератаку (1,1 миллиона долларов США)».

Почти 80% респондентов назвали адаптивный контроль доступа необходимым для снижения угроз кибербезопасности без снижения производительности. Респонденты также высоко оценили строгую аутентификацию перед доступом к данным и приложениям в облаке, а также поддержку нескольких стандартов федерации удостоверений, включая SAML.

Респонденты сообщили об использовании инструментов управления идентификацией и доступом, многофакторной аутентификации и различных решений для анализа угроз для дальнейшего снижения рисков.

Интересно, что наиболее популярными инструментами среди респондентов, вероятно, были также самые основные инструменты безопасности, такие как брандмауэры и защита от вредоносных программ. Даже с ограниченным бюджетом и ограниченным персоналом организации могут значительно повысить уровень безопасности, внедрив базовые меры безопасности наряду с инструментами предотвращения и обнаружения.

Знание того, что кибератаки могут поставить под угрозу безопасность пациентов и повлиять на лечение, является более чем достаточной причиной для срочного приоритета кибербезопасности в здравоохранении». ***(Jill McKeon. How Healthcare Cyberattacks Can Impact Patient Safety, Care Delivery // TechTarget, Inc. (https://healthitsecurity.com/news/how-healthcare-cyberattacks-can-impact-patient-safety-care-delivery). 08.09.2022).***

***

«Половина всех автомобильных кибератак в истории произошла только в 2021 году, что почти на 140% больше, чем в 2020 году.

Об этом сообщает Upstream Security Ltd., стартап, предлагающий облачную платформу автомобильной кибербезопасности и аналитики данных, которая открывает свой первый операционный центр безопасности транспортных средств за пределами своего родного Израиля в Анн-Арборе, штат Мичиган.

Количество подключенных автомобилей на дорогах резко возросло, и автопроизводители, в том числе Детройтская тройка, планируют добавить еще миллионы в течение оставшейся части десятилетия, предлагая беспроводные обновления, функции по запросу и технологические преимущества, которые требуются клиентам.

Это, однако, также означает, что они могут быть уязвимы для кибератак, которые могут украсть личную информацию, получить контроль над функциями автомобиля и даже потенциально предоставить хакерам доступ к большей электрической сети. И эти угрозы растут: в 2022 году на автопроизводителей и поставщиков интеллектуальной мобильности приходится 6% целей атак по сравнению с 2% в прошлом году.

«Автомобильная промышленность сейчас находится на этапе, когда автомобили, грузовики и транспортные средства действительно становятся просто еще одним устройством», — сказал Ричард Форно, заместитель директора Центра кибербезопасности Университета Мэриленда, округ Балтимор. «У вас есть смартфоны, Amazon Alexas, автомобили теперь просто еще одно интеллектуальное устройство. Таким образом, они всегда подключены к сети. Существует ряд проблем с безопасностью для любого другого постоянно включенного устройства. будет наблюдаться увеличение количества атак».

Вот тут-то и появляется Upstream. Работая с автопроизводителями, он предлагает уровень защиты для выявления злоумышленников и борьбы с ними, что является требованием регулирования услуг, — говорит генеральный директор Йоав Леви.

«Это критически важная инфраструктура, к которой должны относиться очень серьезно не только автомобильные компании или владельцы автопарков, — сказал он, — но и правительство».

По словам Леви, хакеры могут запрашивать личную информацию, такую как номера кредитных карт, чтобы разблокировать и запустить транспортные средства для кражи, а также получить доступ к станциям зарядки электромобилей для установки программ-вымогателей, отключить их в качестве средства кибервойны или даже получить доступ к большей электросети. Кроме того, существует вероятность нарушения цепочек поставок, доставки и других услуг.

«Воздействие гораздо больше, чем если бы кто-то владел предприятием и украл их данные», — сказал Леви. «Ущерб бренду очень большой».

Кроме того, по его словам, транспортные средства более уязвимы, когда они используют общедоступные зарядные станции или получают беспроводные обновления, которые быстро расширяются в отрасли.

По его словам, Upstream может покрыть 90% потенциальных атак на транспортное средство. От своих клиентов он получает информацию, поступающую от подключенных транспортных средств, зарядных станций и других цифровых приложений, которые собираются в облаке. Платформа Upstream выполняет анализ безопасности и использует модели машинного обучения для поиска известных и неизвестных аномалий в данных.

У компании есть сотни сценариев, созданных на основе различных вариантов использования, когда обнаруживаются аномалии и действия, которые можно

предпринять для защиты транспортного средства или информации. В зависимости от типа атаки некоторые действия выполняются автоматически, другие могут занять больше времени. Действия также могут включать отключение SIM-карты в автомобиле, взаимодействие с командой автопроизводителя по кибербезопасности и обращение к водителю.

«Мы обеспечиваем обзор всего флота с высоты птичьего полета», — сказал Леви. «И за этим наблюдают эксперты по кибербезопасности. Как только они обнаружат угрозу или аномалию, они смогут отреагировать практически в режиме реального времени с помощью плейбуков и фактически снизить риск».

Таким образом, Upstream смогла предложить защиту не только новым транспортным средствам, но и существующим подключенным транспортным средствам, уже находящимся в пути, что было одной из целей компании при ее запуске в 2017 году.

Сегодня Upstream отслеживает около 12 миллионов автомобилей. Его центр в Анн-Арборе будет отвечать за несколько миллионов долларов.

Леви отказался уточнить, работает ли Upstream с одним из автопроизводителей Детройта, сославшись на деликатный характер кибербезопасности. Однако за четыре финансовых раунда компания получила более 100 миллионов долларов. В число сторонников входят альянсы Renault, Nissan и Mitsubishi, Volvo Group, BMW и Hyundai Motor Co., а также страховые компании, транспортные компании и другие инвесторы. Леви отказался обсуждать финансовые детали фирмы.

Центр в Анн-Арборе будет работать круглосуточно и без выходных. Upstream обучает 10 человек для центра, но нанимает как на полный, так и на неполный рабочий день. Сегодня в компании работает 130 сотрудников по всему миру. Леви рекомендует степень информатики для тех, кто интересуется работой, хотя это не требуется для работы.

Компания Upstream выбрала Анн-Арбор для доступа к клиентам и базе автомобильных знаний Юго-восточного Мичигана. В Израиле, где граждане обязаны проходить военную службу, многие люди имеют опыт в области кибербезопасности, и Upstream предлагает обучение ее применению для автомобилей.

В Мичигане все наоборот. Upstream надеется извлечь выгоду из глубоко укоренившихся знаний отрасли в штате и предлагает для нее обучение работе в области кибербезопасности.

«Мы можем многому у них научиться благодаря их глубокому опыту в области автомобилестроения, — сказал Леви. «У нас нет автомобильной компании в Израиле, которая производит автомобили, поэтому наши познания в автомобилестроении очень узки».

Центр является еще одним свидетельством того, что опыт Мичигана в автомобильном транспорте дает ему преимущество для развития экосистемы, поддерживающей автомобили будущего.

«Компании продолжают инвестировать в Мичиган из-за наших талантов мирового класса, качества жизни, низкой стоимости ведения бизнеса и культуры инноваций», — заявил Тревор Пол, главный специалист по мобильности Мичигана. «Мичиган по-прежнему стремится стать глобальным эпицентром следующей

революции в автомобильной промышленности, и мы приветствуем продолжающийся успех Upstream и инвестиции в автономное и электрифицированное будущее Мичигана».

Upstream ожидает, что ее центр в Анн-Арборе будет полностью введен в эксплуатацию к концу года. Он также хочет открыть операцию по обеспечению безопасности транспортных средств в центре Японии». ***(Breana Noble. This company aims to protect connected cars from cyberattacks // Tech Xplore (https://techxplore.com/news/2022-09-company-aims-cars-cyberattacks.html). 07.09.2022).***

***

«Один из ключевых компонентов мировой торговли также является одним из наиболее уязвимых для угроз кибербезопасности, и если такая атака окажется успешной, она вызовет огромные сбои с эффектом домино для людей во всем мире.

По данным Конференции Организации Объединенных Наций по торговле и развитию (ЮНКТАД), более 80% объема международной торговли товарами осуществляется по морю, и этот процент еще выше для развивающихся стран.

Вся отрасль зависит от ряда сложных цепочек поставок «точно в срок». если хотя бы один элемент нарушен, это может иметь серьезные последствия.

Один пример: сбой в цепочках поставок по всему миру в 2021 году, когда один из крупнейших существующих контейнеровозов Ever Given сел на мель в Суэцком канале, заблокировав один из самых загруженных судоходных каналов в мире и вынудив многие другие суда ждать гораздо дольше. путешествия вокруг мыса Доброй Надежды, что серьезно задерживает поставки электроники, машин, мебели, товаров для дома и многого другого.

Порты и судоходство все больше подключаются к Интернету, и это делает их заманчивой мишенью для хакеров, особенно когда большая часть сектора одновременно зависит от устаревших технологий, которым может быть несколько десятков лет.

И перспектива разрушительных кибератак на судоходство и порты не просто теоретическая — они уже происходят.

В 2017 году судоходному гиганту Maersk пришлось столкнуться с отставанием в портах, когда он пострадал в результате глобальной кибератаки NotPetya. Компании пришлось переустановить тысячи серверов и десятки тысяч ПК, чтобы снова начать работу.

В 2021 году крупная кибератака нарушила контейнерные операции в южноафриканском порту Кейптаун, ограничив движение грузов до тех пор, пока системы не будут восстановлены. Оба инцидента, наряду с остановкой Ever Given, демонстрируют, как сбои в доставке могут иметь серьезные последствия для глобальной цепочки поставок, предприятий и частных лиц.

Несмотря на это, морская отрасль остается недостаточно подготовленной к кибератакам.

«Это действительно большая область, измеряемая триллионами долларов, но это также своего рода старая гвардия в том смысле, что ничего не происходит, ничего

не меняется очень быстро», — говорит Кевин Джонс, профессор компьютерных наук в Университете Плимута и руководитель в Исследовательской группе по морским киберугрозам.

«И есть мышление в секторе «Как только я покину порт… никто не сможет меня тронуть, мне не нужно ни о чем беспокоиться, пока я не вернусь». Эти вещи были правдой 30 или 40 лет назад, но они больше не соответствуют действительности».

Такой подход означает, что отрасль изо всех сил пытается идти в ногу с угрозами кибербезопасности, с устаревшими ИТ-системами и отсутствием информации о сетях, что делает ее главной целью для хакеров, и это может иметь далеко идущие последствия.

В совместном с Банком Англии проекте, призванном проверить, как страховые компании отреагируют на такой инцидент, Исследовательская группа морских киберугроз Плимута разработала сценарий, в котором злоумышленники тайно получают контроль над средствами управления кораблем и используют это, чтобы врезаться в порты и краны, нанося ущерб корабли и инфраструктура, а также потеря груза.

В этом вымышленном сценарии злоумышленники также угрожают вызвать новые аварии, если пять крупнейших судоходных компаний не заплатят выкуп в размере 50 миллионов долларов каждая. Чтобы предотвратить дальнейшие атаки, большая часть судоходства в мире останавливается на несколько дней, что наносит ущерб глобальной цепочке поставок.

Это воображаемое событие, но оно основано на наихудших сценариях того, чего злоумышленники могут достичь, нацелившись на отрасль, которая изо всех сил пытается не отставать от кибербезопасности, — в то время, когда киберкомандование береговой охраны США предупредило о 68-процентном росте сообщений о кибербезопасности. инцидентов в секторе только за последний год.

Частично проблема заключается в необычном характере операционной среды: управление технологией на огромном контейнеровозе — это совсем другая ситуация, чем работа с компьютерами в офисе. Когда судно может находиться в океане неделями или месяцами, полное обновление ИТ-систем не может быть выполнено в кратчайшие сроки, а отсутствие подключения может затруднить загрузку исправлений безопасности и обновлений программного обеспечения, даже критических. те.

«Сегодняшнее состояние морской отрасли с точки зрения кибербезопасности довольно плохое, и это связано не только с владельцами и операторами отрасли, но и со сложностью», — говорит Том Скривен, главный консультант компании по кибербезопасности Mandiant, который ранее провел восемь лет на флоте.

Он отмечает, что есть проблемы с устаревшими системами, а также с появлением новых кораблей, которые имеют расширенные возможности подключения, что приводит к новым проблемам, таким как отсутствие сегментации во внутренних сетях, увеличение поверхности угроз со стороны третьих сторон и поставщиков, а также подключение клиентов. туда и обратно, говорит он.

Все эти факторы помогают сделать морские суда главной мишенью для хакеров с самыми разными мотивами, начиная от кибершпионажа и заканчивая получением прибыли от киберпреступлений.

Скривен указывает на хакерскую группу, которую Mandiant отслеживает как APT40, которая представляет собой операцию по кибершпионажу, связанную с китайским государством, которая нацелена на машиностроение, транспорт и оборонную промышленность, особенно там, где эти сектора пересекаются с морскими технологиями. Группа проводила операции по крайней мере с 2013 года, что, по словам исследователей, является средством поддержки усилий Китая по модернизации своего флота путем изучения систем и кражи конфиденциальных чертежей.

Mandiant также подробно рассказал о нападениях киберпреступников на израильский судоходный сектор. Предполагается, что это работа хакеров, действующих из Ирана с целью шпионажа и сбора разведывательных данных в поддержку иранских интересов. Атаки включают маскировку под законные облачные сервисы для кражи имен пользователей и паролей, а также попытки обманным путем заставить жертв загрузить вредоносное ПО.

Тогда есть киберпреступники, которые действуют из-за финансовой выгоды. Эти хакеры хотят заработать как можно больше денег с наименьшими усилиями — и нацеливание на морскую отрасль может принести им большую зарплату из-за сочетания старых, небезопасных сетей и того факта, что портовая инфраструктура жизненно важна для многих. отрасли.

«Если бы вы нашли оператора или поставщика аналогичного размера в европейской экосистеме — возможно, работающего в Роттердаме, Антверпене или Феликстоу, — и тогда вы добились бы того же успеха, что и злоумышленник, — последствия восьми дней серьезного движения поврежденных контейнеров, воздействие на и без того перегруженную цепочку поставок было бы ужасающим», — говорит Скривен.

Но кибератаки на морскую отрасль могут нарушить работу не только портов. Существует также вероятность того, что, нацелившись на нужные системы, киберпреступники могут предоставлять кораблям в открытом море недостоверную информацию, вмешиваться в их GPS-трекинг или давать ложные предупреждения, которые могут сбить корабли с курса — либо для того, чтобы вызвать сбои, либо для того, чтобы направить их. навстречу неприятностям или даже пиратам, которые хотят увести цели с морских путей в менее защищенные районы.

Это может показаться надуманным, но такого рода сбои представляют собой вполне реальную угрозу, особенно во время конфликтов.

«К этому нужно относиться очень и очень серьезно, потому что последствия крупного инцидента могут быть огромными, особенно во время конфликта», — говорит капитан Рахул Ханна, глобальный руководитель отдела морских консультаций в Allianz и ветеран с 14-летним стажем работы в море. «Мы уже видели, что спуфинг GPS имел место, это происходит, и мы просто надеемся, что в конфликте между странами нет побочного ущерба. В целом отрасль должна понять, что нам нужно извлечь уроки из этого».

В настоящее время реализуются инициативы, направленные на улучшение кибербезопасности в секторах морского и судоходства, такие как программа Международной морской организации по защите от морских киберрисков. Он направлен на предоставление руководящих принципов, которые позволяют производителям судов, судоходным компаниям и портам выявлять, анализировать и оценивать киберриски и снижать их до приемлемого уровня для обеспечения безопасного и надежного судоходства.

Но по большей части это руководящие принципы — и с кораблями, системами, которые их приводят в действие, и даже устройствами, подключенными к Интернету вещей, внутри современных судов, которые производятся в разных странах с разным уровнем регулирования, это далеко не так. вверх. Эта ситуация должна измениться, прежде чем ситуация может улучшиться.

«Отрасль в целом должна понять, что мы должны извлечь из этого уроки, и это только вопрос времени, когда кто-то действительно подвергнется нападению, поэтому необходимо обеспечить соблюдение нормативных требований, особенно в критических частях отрасли, которые могут оказывают гораздо большее влияние», — говорит Кханна.

Как и в любой другой отрасли, базовые элементы могут значительно помочь в повышении безопасности, например, применение исправлений безопасности, использование надежных паролей и развертывание многофакторной аутентификации. Природа доставки означает, что труднее найти время для обеспечения этой поддержки информационной безопасности при перевозке грузов по всему миру, но забота о безопасности в долгосрочной перспективе более выгодна, чем оставлять ее в стороне.

Именно такие вещи обсуждает Исследовательская группа по морским киберугрозам Университета Плимута с производителями судов, а также с капитанами кораблей, поскольку, в конечном счете, они несут ответственность за безопасность инфраструктуры, когда они находятся на высоте. моря.

«Базовая осведомленность о кибербезопасности, осуществляемая с учетом контекста, имеет огромное значение, наряду с установлением надлежащих протоколов», — говорит Джонс. «Часть этого заключается в том, чтобы знать, когда делать такие вещи, как исправление, а когда заменять многое, — это знать, каков ваш риск».

«Должны ли вы исправлять в пути? Ответ, вероятно, «да», если это критическое исправление, если вы знаете, что делаете. на самом деле потому, что в этот момент риск как бы перевешивает вознаграждение», — объясняет он.

Джонс и другие надеются, что попытки привлечь внимание к проблемам кибербезопасности в морском секторе побуждают к действиям, повышая устойчивость отрасли, которая имеет большое значение, особенно для глобальных цепочек поставок. чем нужно иметь дело с после того, как они произошли…» ***(Danny Palmer. This overlooked cybersecurity risk could create an ocean of trouble for us all // ZDNET (https://www.zdnet.com/article/this-overlooked-cybersecurity-risk-could-create-an-ocean-of-trouble-for-us-all/). 06.09.2022).***

***

«Хотя Интернет, несомненно, принес новые преимущества, он также принес новые проблемы, поскольку киберпреступники пытаются использовать нашу, казалось бы, постоянно растущую зависимость от возможности подключения.

Фишинговые электронные письма, атаки вредоносных программ и программ-вымогателей, кражи ваших банковских реквизитов, паролей и другой личной информации — Интернет предоставил злонамеренным хакерам множество новых способов заработать деньги и вызвать сбои. Просто посмотрите, например, как критическая инфраструктура, школы и больницы пострадали от кибератак.

Нам еще предстоит полностью защитить сети от современных интернет-угроз, но технологии уже развиваются, создавая новые угрозы, к которым мы должны как-то подготовиться.

Quantum: взлом и майнинг криптовалют

Одним из наиболее значительных технологических прорывов, стоящих на нашем пути, являются квантовые вычисления, которые обещают быстро решать сложные задачи, которые побеждали классические компьютеры.

Хотя этот прогресс принесет пользу научным исследованиям и обществу, он также создаст новые проблемы. В частности, мощь квантовых вычислений может быстро взломать алгоритмы шифрования, которые мы использовали на протяжении десятилетий для защиты целого ряда областей, включая онлайн-банкинг, безопасные коммуникации и цифровые подписи.

В настоящее время квантовые вычисления дороги, а опыт, необходимый для их разработки, ограничен крупными технологическими компаниями, исследовательскими институтами и правительствами. Но, как и любая инновационная технология, со временем она станет более доступной и доступной, и киберпреступники будут стремиться воспользоваться преимуществами квантовой технологии.

«Есть некоторые вещи на горизонте, которые вы можете предвидеть; в частности, квантовые вычисления, способные взломать существующие алгоритмы шифрования», — говорит Мартин Ли, технический руководитель отдела исследований в области безопасности в Cisco Talos.

«То, что было вполне подходящей длиной ключа шифрования 20 лет назад, больше не подходит».

Агентство США по кибербезопасности и безопасности инфраструктуры (CISA) уже предупредило, что необходимо принять меры для защиты сетей от кибератак, основанных на квантовых вычислениях, особенно тех, которые поддерживают критически важную национальную инфраструктуру.

Но хотя разрушительные кибератаки, основанные на квантовых вычислениях, представляют собой ключевую угрозу кибербезопасности будущего, квантовые компьютеры сами по себе могут стать прибыльной целью хакеров.

Давайте подумаем о конкретном примере вредоносного ПО для криптомайнинга. Это форма вредоносного ПО, которое злоумышленники устанавливают на компьютеры и серверы, чтобы тайно использовать мощность чужой сети для добычи криптовалюты и получения прибыли — и все это без необходимости платить за ресурсы или потребляемую мощность.

Криптовалюты, такие как биткойн, генерируются компьютерами путем решения сложных математических задач — таких математических задач, которые могут быть относительно тривиальными для решения сети квантовых компьютеров. Это означает, что если бы киберпреступники смогли внедрить вредоносное ПО для криптомайнинга в квантовые компьютеры, они могли бы очень быстро разбогатеть — почти бесплатно для себя.

«Заражение одного из них позволит кому-то начать вычислять очень сложные алгоритмы», — говорит Дэвид Санчо, старший исследователь антивирусов в Trend Micro.

«Если у вас есть крипто-майнер на квантовом компьютере, это значительно ускорит ваши возможности майнинга — такие вещи становятся целью тривиальных кибератак, это очень легко сделать».

Использование ИИ и машинного обучения

Но квантовые вычисления — не единственная новая технология, которой киберпреступники будут стремиться воспользоваться: мы можем ожидать, что они также будут использовать разработки в области искусственного интеллекта (ИИ) и машинного обучения (МО).

Как и квантовые вычисления, ИИ и машинное обучение, похоже, будут способствовать инновациям в ряде областей, включая робототехнику и беспилотные автомобили, распознавание речи и языка, здравоохранение и многое другое.

ИИ, который может адаптироваться и обучаться, можно использовать во благо, но в конечном итоге, когда он станет более широко доступным, киберпреступники начнут использовать его для повышения эффективности кибератак — это лишь вопрос времени.

«Мы увидим, как кампании с использованием вредоносного ПО, операции с программами-вымогателями и фишинговые кампании будут проводиться полностью автоматически с помощью платформ машинного обучения. Это еще не сделано, но сделать это будет несложно», — говорит Микко Хиппонен, главный исследователь сотрудник WithSecure.

Одним из средств использования этой технологии может быть программирование текстового алгоритма генерации для отправки и ответа на распространенные электронные письма со спамом или кампании компрометации деловой электронной почты (BEC).

Вместо того, чтобы требовать от человека времени для написания и ответа на сообщения, преступники могли бы положиться на алгоритм, который также может анализировать, какие ответы, скорее всего, будут настоящими жертвами, на которых стоит ответить, а не людьми, которые остаются неубежденными, или теми, кто которые отправляют ответы на розыгрыш спамеру. Эта реальность означает, что в будущем вас может обмануть бот.

Существует также вероятность того, что киберпреступники могут использовать достижения в области машинного обучения для разработки самопрограммируемого интеллектуального вредоносного ПО, которое, вместо того, чтобы нуждаться в поддержке разработчика, могло бы обновлять себя, автоматически реагируя на средства киберзащиты, с которыми оно сталкивается, чтобы иметь наибольшие шансы быть эффективными.

«Вы можете себе представить, когда самопрограммирующиеся программы станут более способными, чем сейчас, когда они смогут завершать функции, созданные людьми — это звучит великолепно, пока вы не добавите в них программу-вымогатель», — говорит Хиппёнен.

«Он может изменить код, сделать его более сложным для понимания, сделать его таким, чтобы каждый раз он был разным, он мог попытаться создать необнаруживаемые версии. Все это технически выполнимо, мы просто еще не видели этого — и я думаю, что мы будет", - предупреждает он.

Дипфейки

Но злоупотребление ИИ для усиления киберугроз — это не просто проблема будущего для Интернета — это уже происходит сейчас, когда глубокое обучение используется для создания дипфейков, то есть видео, которые выглядят как реальные люди или события, но на самом деле фальшивый.

Их использовали в кампаниях по политической дезинформации, розыгрышах, чтобы одурачить политиков, и они уже используются для усиления BEC и других мошеннических атак, когда киберпреступники используют дипфейковые аудио, чтобы убедить сотрудников разрешить значительные финансовые переводы на счета, принадлежащие злоумышленникам.

«Мы вступаем в этот дивный новый мир вокруг дипфейковых видео, которые будут использоваться для совершения преступлений. Не только для манипуляций, но и для дезинформации и дезинформации», — говорит Тереза Пэйтон, генеральный директор Fortalice Solutions и бывший ИТ-директор в Белом доме.

Возьмем пример руководителей, которые находятся в публичной сфере. Они появляются по телевидению, произносят речи, есть видео с ними в Интернете, так что найти записи того, как они звучат, относительно просто — и мошенники уже могут использовать эти ресурсы с помощью технологии дипфейка, чтобы имитировать их голос.

В конце концов, если сотруднику звонит глава компании и говорит ему что-то сделать, он, скорее всего, это сделает — и киберпреступники, стоящие за этими атаками, знают об этом факте.

«Мне уже известно о трех случаях, когда дипфейк-аудио использовалось, чтобы успешно убедить кого-то перевести деньги туда, куда они не должны были переводить их», - говорит Пэйтон.

И поскольку технология, стоящая за дипфейками, продолжает совершенствоваться, это означает, что становится все труднее отличить правду от подделки.

«Меня все больше беспокоит отсутствие у нас возможности по-настоящему пресечь манипулятивные кампании, — говорит Пэйтон.

Интернет скомпрометированных вещей

Дипфейки — не единственная область, в которой киберугрозы могут повлиять на нашу повседневную жизнь, если будущее Интернета не защищено должным образом. Интеллектуальные устройства Интернета вещей (IoT) все чаще становятся частью нашей повседневной жизни, поскольку в домах, офисах, на фабриках и т. д. появляются различные датчики, бытовые приборы, носимые устройства и другие подключенные продукты.

Хотя есть определенные преимущества в подключении устройств IoT к нашим домашним и рабочим сетям, этот повышенный уровень сети также создает большую поверхность для атак, которую киберпреступники могут попытаться использовать.

«Когда вы добавляете функциональные возможности и возможности подключения к повседневным устройствам, они становятся уязвимыми для взлома. Устройства, которые невозможно было взломать, становятся доступными для взлома. Это может быть очень сложно. Тем не менее, это всегда выполнимо.

«Это то, что происходит сейчас, в наше время, и это не остановить. Неважно, что мы об этом думаем, это все равно произойдет, и это будет все более незаметно».

Подумайте о своей бытовой технике: все чаще она «умная» и подключена к Интернету. Все, от вашего телевизора до зубной щетки, теперь может быть подключено к Интернету.

Но для производителей бытовой техники создание подключенных к Интернету устройств — относительно новое явление, и многим раньше не приходилось думать об угрозах кибербезопасности. Некоторые поставщики могут вообще не думать об этом в процессе проектирования, оставляя продукты уязвимыми для хакеров.

Хотя хакеры, охотящиеся за вашей кофеваркой или аквариумом, могут не вызывать беспокойства, это точка в сети, к которой можно получить доступ и которую можно использовать в качестве шлюза для атаки на более важные устройства и конфиденциальные данные.

Хотя безопасность IoT должна (надеюсь) улучшаться по мере того, как она становится более распространенной, есть еще одна проблема, которую следует учитывать. Уже существуют миллионы и миллионы устройств IoT, которым не хватает безопасности, и они могут даже не поддерживаться обновлениями безопасности.

Подумайте о том, сколько смартфонов не могут получать обновления безопасности уже через несколько лет. Затем масштабируйте эту реальность до быстрорастущего IoT — что произойдет, если устройства, которые не заменяются регулярно, такие как холодильник или автомобиль, смогут продолжать использоваться десятилетиями?

«На планете нет поставщика программного обеспечения, который поддерживал бы программное обеспечение, написанное 20 лет назад. Этого просто не происходит», — говорит Хиппёнен, который предлагает, когда производители больше не поддерживают обновления для своих устройств, они должны открыть его исходный код, чтобы позволить другим делать это.

«Вы получите исправления безопасности для своих старых, устаревших вещей, заплатив за услугу так же, как вы платите за любую другую услугу».

Подключенные устройства уже становятся повсеместными в обществе, и нет никаких признаков того, что эта тенденция замедлится — целые умные города станут нормой. Но если кибербезопасность и соблюдение нормативных требований не являются ключевой движущей силой этой тенденции, это может привести к негативным последствиям для всех.

«Если вы не решите эти проблемы, атаки будут происходить с такими масштабами и скоростью, которых вы никогда раньше не видели, — плохие вещи будут происходить быстрее. Это невероятно беспокоит», — говорит Пэйтон, которая

считает, что это всего лишь Вопрос времени, когда программа-вымогатель возьмет в заложники умный город.

«Они станут мишенью, и мы столкнемся с определенным уровнем устойчивых нарушений», — добавляет она.

Гонка вооружений в области кибербезопасности

Несмотря на потенциальные угрозы на горизонте, Пэйтон с оптимизмом смотрит в будущее Интернета. В то время как киберпреступники будут использовать новые технологии для улучшения своих атак, те, кто отвечает за защиту сетей, также будут использовать те же технологии для предотвращения атак.

«Я очень воодушевлена нашей продолжающейся способностью моделировать гнусное поведение, а затем использовать искусственный интеллект, большие данные, аналитику и различные типы алгоритмов машинного обучения для дальнейшего совершенствования технологий», — объясняет она.

«Теперь будет ли он блокировать все? Нет, потому что киберпреступники всегда адаптируют свою тактику. Но у меня есть большой оптимизм в отношении того, что я смогу блокировать больше угроз от базовых до средних, которые, кажется, сегодня проходят.»

Это чувство оптимизма разделяет Хиппёнен, который оглядывается на то, как развивались технологии в последние годы. Он считает, что кибербезопасность улучшается, и что даже с появлением новых технологий это не означает, что киберпреступникам и другим злонамеренным хакерам будет легко.

«Компьютерная безопасность никогда не была в лучшей форме, чем сегодня. Это противоречивый комментарий — люди на улице, скорее всего, подумают, что безопасность данных никогда не была хуже, потому что они видят только сбои. Они видят только заголовки об очередном взломе», он говорит.

«Но дело в том, что если вы сравните безопасность наших компьютеров сегодня и десять лет назад, это как день и ночь. Мы становимся намного лучше в плане безопасности — злоумышленникам гораздо труднее пробиться».

Будем надеяться, что ситуация останется такой же – от того, насколько она верна, зависит будущая стабильность интернета». ***(Danny Palmer. The scary future of the internet: How the tech of tomorrow will pose even bigger cybersecurity threats // ZDNET (https://www.zdnet.com/article/the-scary-future-of-the-internet-how-the-tech-of-tomorrow-will-pose-even-bigger-cybersecurity-threats/). 13.09.2022).***

***

«ИТ-системы InterContinental Hotels Group, крупной гостиничной организации, которая управляет 17 гостиничными брендами по всему миру, были скомпрометированы, что привело к постоянным сбоям в работе систем онлайн-бронирования и других служб корпорации.

IHG, штаб-квартира которой находится в Денхэме, Англия, и офисы в Атланте, Сингапуре и Шанхае, заявила во вторник в заявлении для Лондонской фондовой биржи, что «части [ее] технологических систем подверглись несанкционированной деятельности». Далее он сообщил, что его деятельность была прервана с понедельника, из-за чего люди, по крайней мере, изо всех сил пытаются бронировать комнаты онлайн.

Представители компании заявили в заявлении, что они приводят в действие свои планы реагирования, уведомляют власти о вторжении и работают с поставщиками технологий. Кроме того, для помощи в расследовании привлекаются эксперты извне IHG.

«IHG работает над тем, чтобы как можно скорее полностью восстановить все системы и оценить характер, масштабы и последствия инцидента», — заявили в корпорации. «Мы будем поддерживать владельцев и операторов отелей в рамках нашего реагирования на продолжающиеся перебои в обслуживании. Отели IHG по-прежнему могут работать и принимать заказы напрямую».

Попытки The Register забронировать номер онлайн через веб-сайт IHG не увенчались успехом, поскольку мы неоднократно сталкивались с сообщением о том, что запрошенная страница не отвечает. Переход по ссылкам на другие страницы сайта был встречен с таким же сообщением, хотя некоторые страницы открывались с задержкой в несколько минут.

Компания разместила сообщение для гостей в верхней части главной страницы, информирующее их о том, что «в настоящее время у вас могут возникнуть проблемы с бронированием нового бронирования, доступом к информации о ваших предстоящих бронированиях и доступом к вашей учетной записи IHG One Rewards».

В сообщении говорится, что компания работает над тем, чтобы решить проблемы как можно быстрее, и предлагает клиентам с вопросами обращаться напрямую в отель.

IHG — это крупная компания, в которой работает 6 028 отелей и 882 897 номеров в более чем 100 странах. В нем работает около 325 000 сотрудников, и в его бренды входят Regent, InterContinental Hotels and Resorts, Crowne Plaza, Holiday Inn и Holiday Inn Express, Candlewood Suites, Atwell Suites и Even Hotels.

IHG не сообщила, была ли атака результатом программы-вымогателя или какой-то другой вредоносной программы. Согласно информации, полученной от ihg[.]com, компания по анализу угроз Hudson Rock сообщила в Твиттере, что по меньшей мере 15 сотрудников IHG и 4030 пользователей внутренней сети были скомпрометированы.

Это не первая кибератака на IHG. Нарушение сетевой безопасности в 2016 году повлияло на компанию примерно на три месяца, а официальные лица IHG признали в апреле 2017 года, что вторжение затронуло 1200 отелей. В этой путанице злоумышленники развернули вредоносное ПО, которое получило доступ к данным платежных карт, которые затем использовались для мошеннических платежей с помощью клонированных карт.

Три года спустя IHG урегулировала предъявленный ей коллективный иск с максимальной суммой в 1,55 миллиона долларов.

Организации гостиничного бизнеса входят в число основных отраслей, на которые нацелены киберпреступники. Mews, производитель систем управления недвижимостью, заявил в своем блоге в прошлом году, что заказы — как онлайн, так и на стойке регистрации — и большое количество кредитных карт, которые они обрабатывают, делают такого рода организации привлекательными и уязвимыми целями. Эти группы также хранят много данных о путешественниках, которые могут быть полезны, скажем, для спецслужб, желающих отслеживать определенных

людей. Типы атак включают трояны, скребки памяти, фишинг и отказ в обслуживании.

В июле отели Marriott заявили, что подверглись третьей кибератаке за четыре года, когда злоумышленники украли 20 ГБ данных, включая информацию о кредитных картах и внутренние документы компании.

По словам Аарона Тернера, технического директора SaaS Protect в фирме по кибербезопасности Vectra, любая компания, являющаяся частью более крупной туристической экосистемы, представляет интерес для опытных хакерских команд.

«Будь то авиакомпания или сеть отелей, эти компании по сути являются банками», — сказал Тернер The Register. «Баллы вознаграждения, которые каждая из этих компаний предлагает своим постоянным клиентам, могут быть использованы для монетизации всех видов подпольной интернет-деятельности. Финансовый контроль, который существует для ограничения движения стоимости за счет использования традиционных валют, часто не существует для вознаграждений. точки.»

Он сказал, что видел, как бонусные баллы используются для целого ряда схем монетизации преступных предприятий, от вознаграждений в казино до повышения класса обслуживания авиакомпаний до баллов за лояльность в отелях.

Они также использовались для «виртуальных валют в игровых экосистемах, даже в ситуациях, когда рекламные акции медицинского страхования использовались в мошеннических целях», — сказал он. «В любое время, когда стоимость может быть переведена в обход традиционных средств контроля за переводом валюты, преступники сосредоточатся на этих системах перевода стоимости». ***(Jeff Burt. Cyberattack brings down InterContinental Hotels' booking systems // The Register (https://www.theregister.com/2022/09/06/ihg_hotels_data_breach/). 06.09.2022).***

***

«Akamai заявила, что перекрыла крупнейшую в истории публично известную распределенную атаку типа «отказ в обслуживании» (DDoS) — нападение на незадачливую восточноевропейскую организацию, скорость которой превысила 700 миллионов пакетов в секунду.

Это последнее цунами трафика произошло в понедельник, согласно бизнесу веб-инфраструктуры, и нам сказали, что киберпреступники, ответственные за более ранний рекордный поток DDoS в июле, также стояли за этим последним. Фактически, во второй раз они нацелились на одного и того же клиента, имя которого Akamai не назвала.

Для сравнения, июльская атака достигла максимальной скорости 659,6 млн пакетов в секунду, при этом организация подвергалась атакам 75 раз в своем основном центре обработки данных. По словам Акамаи, на этой неделе пиковая скорость составила 704,8 млн пакетов в секунду, и 201 раз он попал в шесть точек по всему миру. Пакеты были в основном UDP в обоих инцидентах, и хотя июльская атака была нацелена на 512 IP-адресов, сентябрьская атака в общей сложности преследовала 1813, как сообщается.

«Командно-административная система атакующих без задержки активировала многоцелевую атаку, которая увеличилась за 60 секунд», — написал Крейг Спарлинг из Akamai.

Представитель Akamai сообщил The Register, что они не могут предоставить более подробную информацию о клиенте из Восточной Европы из соображений безопасности.

Бизнес также отказался комментировать ботнет и/или киберпреступников, стоящих за атакой, но раздел «дополнительная информация» в нижней части блога направляет читателей к двум предупреждениям CISA. В одном из них обсуждается, как смягчить спонсируемые российским государством угрозы критически важной инфраструктуре, а во втором представлен более общий обзор гнусной онлайн-деятельности России.

Поскольку незаконное вторжение России в Украину продолжается, становится ясно, что российские команды получают удовольствие от DDoS-атак против своих вражеских правительств и корпораций.

Akamai считает, что его платформа Prolexic, которая включает в себя 20 центров очистки трафика с высокой пропускной способностью по всему миру, предотвратила наводнения DDoS, и заявила, что ее офисы в Гонконге, Лондоне и Токио закрыли

Старая проблема с потенциалом стать ядерной

Читатели Register должны быть прощены, если DDoS-атака на этой неделе вызовет чувство дежа вю, поскольку эти рекордные события безопасности происходят все чаще.

Компания по обеспечению безопасности Radware задокументировала 203-процентное увеличение [PDF] числа предотвращенных DDoS-атак на одного клиента в течение первых шести месяцев 2022 года по сравнению с первыми шестью месяцами прошлого года и рост на 239 процентов по сравнению с последними шестью месяцами прошлого года. 2021.

Также в прошлом месяце Google заявила, что заблокировала крупнейшую в истории DDoS-атаку на основе HTTPS в июне, пик которой составил 46 миллионов запросов в секунду.

Это, как отметил облачный гигант, было примерно на 76 процентов больше, чем предыдущая рекордная DDoS-атака, которую Cloudflare предотвратила ранее в том же месяце. Кроме того, это последовало за еще одним (на тот момент) рекордным сетевым флудом, который Cloudflare растоптал в апреле.

Тот факт, что одна и та же организация снова стала целью рекордной атаки, указывает на то, что между злоумышленником и жертвой развивается гонка вооружений DDoS, так же как и физический конфликт. Соперничество между защитниками анти-DDoS также продолжается». ***(Jessica Lyons Hardcastle. Eastern European org hit by second record-smashing DDoS attack // The Register (https://www.theregister.com/2022/09/16/record_european_ddos_attack_akamai/). 16.09.2022).***

***

«Один из крупнейших операторов общественного транспорта Великобритании Go-Ahead Group стал жертвой кибератаки. Go-Ahead Group, которая соединяет людей через свои автобусные и железнодорожные сети, сообщила, что «управляет инцидентом кибербезопасности» после того, как в ее сети была обнаружена «несанкционированная активность».

Этот тип кибератаки на транспортную систему Великобритании не редкость. В течение некоторого времени хакеры регулярно атаковали авиационную отрасль. По замыслу кибератаки нацелены на прерывание поездок и кражу больших объемов критически важных данных о клиентах и сотрудниках.

Необходимость автономного ответа

В настоящее время все организации ежедневно борются с более чем миллиардом киберугроз. Чтобы транспортные компании продолжали работать, они должны постоянно оглядываться на подобные атаки. Только приняв автономный ответ на киберзащиту, транспортные операторы могут реагировать с высокой скоростью, чтобы гарантировать, что они не пропустят атаку.

Кроме того, принцип нулевого доверия позволяет ИТ-командам постоянно проверять и оценивать риски, чтобы они могли выявлять кибератаки и противостоять им до того, как они войдут в экосистему организации. Это упрощается при включении контекста, такого как устройство, сетевое местоположение и геолокация, чтобы иметь полный контроль над доступом пользователей. Именно это целостное представление даст операторам поездов информацию о приближении нападения.

Растянуто за пределы возможностей

Согласно отчету Censornet «Средний рынок Великобритании о Code Red Report», в команде почти семи из десяти (69%) организаций среднего размера есть три человека или меньше, которые занимаются вопросами кибербезопасности. Это означает, что каждый десятый (11%) не имеет времени или возможностей для изучения 50% предупреждений, которые он получает каждый день.

Эта неспособность реагировать на киберугрозы усугубляется неуправляемым портфелем точечных продуктов, которые использует большинство организаций. В прошлом году организации среднего размера обычно использовали в среднем продукты с 24 баллами. Это множество продуктов кибербезопасности, которые необходимо отслеживать.

Переход к платформенному подходу

В настоящее время организации отказываются от использования дорогостоящих и трудоемких разрозненных точечных продуктов, принимая платформенный подход. Это помогает обеспечить автономное реагирование на кибератаки, сокращая ручное вмешательство и обеспечивая максимально возможную прозрачность в отношении всех входящих угроз.

Важно отметить, что это дает группам безопасности больше времени для расследования киберпредупреждений и предотвращения атак, подобных этим, от прорыва киберзащиты организации». ***(Ed Macnair. Go-Ahead cyberattack might derail UK public transport services // Help Net Security (https://www.helpnetsecurity.com/2022/09/06/go-ahead-cyberattack/). 06.09.2022).***

***

«Исследователи в области безопасности выявили новые виды кибершпионажа, направленные против правительственных организаций в Азии, а также государственных аэрокосмических и оборонных компаний, телекоммуникационных компаний и ИТ-организаций.

Группа угроз, стоящая за этой активностью, представляет собой отдельный кластер, ранее связанный с RAT «ShadowPad» (троян удаленного доступа). В недавних кампаниях злоумышленник использовал гораздо более разнообразный набор инструментов.

Согласно отчету команды Symantec Threat Hunter, в котором подробно рассказывается об этой деятельности, атаки по сбору разведывательных данных осуществляются как минимум с начала 2021 года и продолжаются до сих пор.

Текущая кампания, по-видимому, почти полностью сосредоточена на правительстве или общественных организациях в Азии, в том числе:

Глава правительства/аппарат премьер-министра

Государственные учреждения, связанные с финансами

Государственные аэрокосмические и оборонные компании

Государственные телекоммуникационные компании

Государственные ИТ-организации

Государственные медиакомпании

Symantec представляет пример атаки, развернувшейся в апреле 2022 года, чтобы продемонстрировать, как шпионская группа компрометирует свои правительственные цели.

Атака начинается с внедрения вредоносной DLL, которая загружается сбоку путем запуска исполняемого файла законного приложения для загрузки файла.dat.

В этом случае законным приложением, которым злоупотребляли хакеры, был исполняемый файл Bitdefender Crash Handler 11-летней давности.

Начальная полезная нагрузка.dat содержит зашифрованный шеллкод, который можно использовать для выполнения команд или дополнительных полезных данных непосредственно из памяти.

Всего через три дня после установления доступа к бэкдору злоумышленники установили ProcDump, чтобы получить учетные данные пользователя из серверной службы Local Security Authority (LSASS).

В тот же день среда тестирования на проникновение LadonGo была снова загружена с помощью перехвата DLL и использована для сетевой разведки.

Через две недели после первоначального вторжения злоумышленники вернулись на скомпрометированную машину, чтобы установить Mimikatz, широко используемый инструмент для кражи учетных данных.

Более того, хакеры попытались использовать CVE-2020-1472 (Netlogon) на двух компьютерах в одной сети, чтобы повысить их привилегии.

Злоумышленники использовали PsExec для запуска Crash Handler и трюка с перехватом порядка DLL для загрузки полезной нагрузки на дополнительные компьютеры в сети.

Через месяц после вторжения злоумышленники получили привилегии для создания новых учетных записей пользователей и смонтировали моментальный

снимок сервера Active Directory для доступа к учетным данным пользователей и файлам журналов.

Наконец, Symantec наблюдала за развертыванием Fscan для попытки эксплуатации CVE-2021-26855 (Proxylogon) против серверов Exchange в скомпрометированной сети.

Одним из инструментов, используемых в атаках в последних кампаниях, является ранее неизвестный похититель информации (Infostealer.Logdatter), фактически заменивший ShadowPad.

Возможности этого нового инструмента включают в себя:

Кейлоггинг

Делаем скриншоты

Подключение к базам данных SQL и запросы к ним

Внедрение кода: чтение файла и внедрение содержащегося в нем кода в процесс.

Загрузка файлов

Кража данных из буфера обмена

Помимо инфостилера и всех инструментов, упомянутых в предыдущем разделе, злоумышленники развернули QuasarRAT, Nirsoft PassView, FastReverseProxy, PlugX, Trochilus RAT и различные скрипты PowerSploit.

Команда Symantec Threat Hunter связала эту кампанию с спонсируемыми китайским государством группами угроз APT41 и Mustang Panda на основе вредоносных инструментов, ранее связанных с этими шпионскими группами.

Например, в кампаниях, приписываемых APT41, наблюдалось использование исполняемого файла Bitdefender для боковой загрузки вредоносного кода.

Symantec также подчеркивает использование того же кейлоггера, развернутого в атаках APT41, против критически важных инфраструктурных организаций, базирующихся в Юго-Восточной Азии.

«Существует ограниченное количество доказательств, позволяющих предположить связи с прошлыми атаками с использованием вредоносного ПО Korplug/PlugX и с атаками ряда известных групп, включая Blackfly/Grayfly (APT41) и Mustang Panda», — заявили исследователи.

Следовательно, вполне вероятно, что за этими шпионскими кампаниями стоят китайские хакеры, но доказательства недостаточно убедительны для уверенной атрибуции.

Чтобы защитить свои системы от изощренных угроз, обновляйте все программное обеспечение, чтобы предотвратить использование известных уязвимостей, и тщательно проверяйте запущенные процессы на всех компьютерах для выявления программных имплантатов.

Все большее число APT внедряют перехват очередей DLL, поэтому любое программное обеспечение, работающее в системах, которое не является частью портфолио организации, является красным флагом, даже если решения безопасности не помечают его как вредоносное». ***(Bill Toulas. Cyberspies drop new infostealer malware on govt networks in Asia // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/cyberspies-drop-new-infostealer-malware-on-govt-networks-in-asia/). 13.09.2022).***

***

«Uber считает, что хакер, стоящий за взломом на прошлой неделе, связан с группой вымогателей Lapsus$, известной тем, что взламывает другие известные технологические компании, такие как Microsoft, Cisco, NVIDIA, Samsung и Okta.

Компания добавила, что злоумышленник использовал украденные учетные данные подрядчика Uber EXT в атаке усталости MFA, когда подрядчик был завален запросами на вход с двухфакторной аутентификацией (2FA), пока один из них не был принят.

Эта тактика социальной инженерии стала очень популярной и использовалась в недавних атаках, нацеленных на известные компании по всему миру, включая Twitter, Robinhood, MailChimp и Okta.

«Оттуда злоумышленник получил доступ к нескольким другим учетным записям сотрудников, что в конечном итоге дало злоумышленнику повышенные права доступа к ряду инструментов, включая G-Suite и Slack», — пояснил Uber в обновлении исходного заявления.

«Затем злоумышленник разместил сообщение в общекорпоративном канале Slack, который многие из вас видели, и перенастроил OpenDNS Uber для отображения графического изображения сотрудникам на некоторых внутренних сайтах».

Компания добавила, что не обнаружила доказательств того, что злоумышленник мог получить доступ к производственным системам, в которых хранится конфиденциальная информация о пользователях, включая личные и финансовые данные (например, номера кредитных карт, информацию о банковских счетах пользователей, личные данные о здоровье или историю поездок).

На данный момент компания расследует инцидент с помощью ФБР и Министерства юстиции США.

«Мы тесно сотрудничаем с ФБР и Министерством юстиции США по этому вопросу и будем продолжать поддерживать их усилия», — добавил Uber.

Uber заявляет, что предпринял некоторые меры для предотвращения будущих нарушений с использованием такой тактики, в том числе:

Мы выявили все учетные записи сотрудников, которые были скомпрометированы или потенциально скомпрометированы, и либо заблокировали их доступ к системам Uber, либо потребовали сброса пароля.

Мы отключили многие затронутые или потенциально затронутые внутренние инструменты.

Мы поменяли ключи (фактически сбрасывая доступ) ко многим нашим внутренним службам.

Мы заблокировали нашу кодовую базу, предотвратив любые новые изменения кода.

При восстановлении доступа к внутренним инструментам мы требовали от сотрудников повторной аутентификации. Мы также продолжаем укреплять наши политики многофакторной аутентификации (MFA).

Мы добавили дополнительный мониторинг нашей внутренней среды, чтобы еще тщательнее следить за любой дальнейшей подозрительной активностью…

Uber добавил, что еще предстоит обнаружить доказательства того, что злоумышленник получил доступ и внедрил какой-либо вредоносный код в свою кодовую базу.

«Прежде всего, мы не видели, чтобы злоумышленник получил доступ к производственным (то есть общедоступным) системам, на которых работают наши приложения, любым учетным записям пользователей или базам данных, которые мы используем для хранения конфиденциальной информации о пользователях, таких как номера кредитных карт, банковские реквизиты пользователей. информация об учетной записи или история поездок. Мы также шифруем информацию о кредитной карте и личные данные о здоровье, предлагая дополнительный уровень защиты», — сказал Uber.

«Мы проверили нашу кодовую базу и не обнаружили, что злоумышленник вносил какие-либо изменения. Мы также не обнаружили, что злоумышленник получил доступ к каким-либо данным клиентов или пользователей, хранящимся у наших облачных провайдеров (например, AWS S3)».

К сожалению, в результате вторжения был получен доступ к некоторой конфиденциальной информации, включая некоторые счета-фактуры Uber из внутреннего инструмента, используемого финансовой командой компании, и отчеты об уязвимостях HackerOne (как сообщил BleepingComputer в пятницу).

«Однако все отчеты об ошибках, к которым злоумышленник смог получить доступ, были исправлены», — заявили в компании. С тех пор HackerOne отключил программу вознаграждения за обнаружение ошибок Uber, тем самым отрезав доступ к раскрытым уязвимостям Uber.

Источник BleepingComputer также сообщил, что злоумышленник смог удалить все отчеты об уязвимостях, прежде чем потерять доступ к программе вознаграждения за обнаружение ошибок Uber, включая отчеты, ожидающие исправления, что представляет серьезную угрозу безопасности для компании.

Было бы неудивительно, если бы субъект угрозы уже выставил эти отчеты об уязвимостях на продажу, чтобы получить прибыль, и чтобы другие субъекты угроз могли использовать их, если они не (полностью) исправлены, в будущих атаках.

Злоумышленник (известный как «teapots2022») также заявил о взломе студии видеоигр Rockstar Games (под псевдонимом «teapotuberhacker») в выходные после утечки игровых видео и скриншотов исходного кода как из Grand Theft Auto V, так и из Grand Theft. Auto VI в качестве доказательства». ***(Sergiu Gatlan. Uber links breach to Lapsus$ group, blames contractor for hack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/uber-links-breach-to-lapsus-group-blames-contractor-for-hack/). 19.09.2022).***

***

«Компания по обеспечению безопасности в Интернете Imperva объявила, что ее решение по предотвращению DDoS-атак (распределенный отказ в обслуживании) побило новый рекорд, защитив от одной атаки, в результате которой одному из ее клиентов было отправлено более 25,3 миллиарда запросов.

Целью был китайский поставщик телекоммуникационных услуг, который часто подвергался DDoS-атакам с необычно большими объемами.

DDoS-атака развернулась 27 июня 2022 года, достигнув пика в 3,9 миллиона запросов в секунду (RPS) и в среднем 1,8 миллиона RPS.

Хотя это меркнет по сравнению с рекордной атакой, которую Cloudflare смягчила в июне, которая превысила 26 миллионов запросов в секунду, продолжительность в случае с Imperva была необычно долгой.

Атаки с пиковым значением более одного миллиона запросов в секунду обычно длятся от нескольких секунд до нескольких минут, но одна атака, которую смягчила Imperva, длилась более четырех часов.

«Атака началась со скоростью 3,1 млн запросов в секунду и поддерживала скорость около 3 млн запросов в секунду. После того, как атака достигла пика в 3,9 млн запросов в секунду, атака снизилась на несколько минут, но вернулась к полной мощности еще на час», — описывает Imperva.

По данным компании, только одна из десяти DDoS-атак длится более часа, и еще меньший процент приходится на такую длительную огневую мощь.

DDoS-атака, которую противодействовала Imperva, была запущена массивным ботнетом, распространившимся по 180 странам, причем большинство IP-адресов находились в США, Бразилии и Индонезии.

Ботнет использовал 170 000 захваченных устройств, включая модемы-маршрутизаторы, интеллектуальные камеры безопасности, уязвимые серверы и плохо защищенные IoT.

Imperva отмечает, что некоторые из серверов, с которых исходил вредоносный трафик, размещены в общедоступных облаках и у поставщиков услуг облачной безопасности, что указывает на крупномасштабное злоупотребление.

Хотя ботнет не был назван или идентифицирован, похоже, что это не Mantis, который был ответственен за отчет Cloudflare по предотвращению DDoS летом.

Cloudflare говорит, что Mantis использует меньшее количество устройств, немногим более пяти тысяч, сосредоточившись в основном на привлечении мощных серверов и виртуальных машин.

Количество устройств, использованных против клиента Imperva, ближе к оценкам Mēris, ботнета, ответственного за предыдущий рекорд DDoS, в 21,8 миллиона RPS. По оценкам исследователей, рой Mēris включает от 30 000 до 250 000 устройств.

Тем не менее, и Mēris, и Mantis ранее наносили быстрые удары короткими вспышками атак, а не многочасовыми DDoS-атаками, так что это может быть новый, еще не идентифицированный ботнет». ***(Bill Toulas. Imperva mitigated long-lasting, 25.3 billion request DDoS attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/imperva-mitigated-long-lasting-253-billion-request-ddos-attack/). 20.09.2022).***

***

«Исследователи из Abnormal Security выявили группировку Chiffon Herring, нацеленную на сотрудников университетов в новых атаках по перехвату заработной платы (Payroll Diversion). Chiffon Herring действует с

марта и в основном нацелена на местные школьные округа и университеты в США. Злоумышленники, предположительно, находятся в Нигерии и Южной Африке.

В рамках атаки киберпреступник выдает себя за преподавателя и отправляет электронное письмо заведующему кафедрой в университете или офисным сотрудникам школьного округа.

В электронном письме злоумышленник от имени преподавателя пишет, что он недавно сменил банк и ему необходимо обновить свои банковские реквизиты. Чтобы создать ощущение срочности, в электронном письме также упоминается, что предыдущая учетная запись станет неактивной до следующего дня выплаты зарплаты. В результате атаки мошенник указывает реквизиты своего счета, чтобы зарплата жертвы поступила на его счет. Согласно анализу, Chiffon Herring также использует инфраструктуру крупнейшего в мире регистратора доменов GoDaddy для отправки писем.

Почти во всех атаках Chiffon Herring предоставляет банковские реквизиты банка Green Dot для перенаправления средств. Счета в этих банках относительно легко открыть, и в основном они связаны с предоплаченными картами.

Карты предоплаты обычно используются в атаках по перехвату заработной платы для получения прямых депозитов за 48 часов до дня выплаты зарплаты. Таким образом, злоумышленник может иметь доступ к перенаправленным средствам в течение нескольких дней, прежде чем жертва обнаружит факт мошенничества.

Для обеспечения защиты от такой атаки нужно обучить всех сотрудников, особенно финансовых и кадровых, обнаруживать признаки фишинговых атак. Кроме того, учреждения и школы также должны внедрить решение для защиты электронной почты, чтобы блокировать вредоносные электронные письма». ***(Университет стал платить зарплату хакеру // SecurityLab.ru (https://www.securitylab.ru/news/533972.php). 20.09.2022).***

***

«…Альянс цифровых граждан (DCA) поделился некоторыми новыми исследованиями, которые он провел в сотрудничестве с экспертом по пиратской рекламе White Bullet и подразделением кибербезопасности Unit 221B. Группа имеет долгую историю публикации исследований по борьбе с пиратством и ранее уже обращала внимание на вредоносное ПО. Несмотря на эти усилия, проблема остается.

Выводы показывают, что 12% всей рекламы на пиратских стриминговых сайтах связаны с вредоносными программами. Кроме того, почти 80% исследованных сайтов показывали хотя бы несколько объявлений о вредоносных программах.

«Пиратские операторы заманивают пользователей на свои сайты, предлагая им «бесплатный контент», включая новейшие фильмы, музыку и телепередачи. Как только они заходят на пиратский сайт, пользователи подвергаются потоку вредоносных объявлений […], которые используют тактику запугивания и другие уловки, чтобы заставить пользователей нажать на них».

«Операторы [пиратства] и вредоносные программы создали нечестивый треугольник с посетителями пиратских сайтов, которые невольно вступили в опасную игру «Пиратская рулетка», доверив свою кибербезопасность злоумышленникам», — говорится в отчете «Нечестивый треугольник».

Расследователи пиратства пострадали от программ-вымогателей

Эти комментарии довольно пугающие, и чтобы подчеркнуть угрозу, исследователи подробно описывают, как они пострадали от атаки программы-вымогателя после посещения пиратского сайта.

«Всего за несколько кликов на пиратском сайте следователи стали жертвами атаки программы-вымогателя, зашифровавшей их компьютерные файлы. Преступники потребовали плату за их разблокировку. Эта киберугроза наблюдалась на нескольких пиратских сайтах».

К счастью, исследователи использовали виртуальные машины, поэтому им ничего не пришлось платить за разблокировку своих тестовых машин. С помощью этих данных и анекдотов они предупреждают общественность держаться подальше от пиратских сайтов.

В целом отчет рисует довольно мрачную картину, предполагая, что дела обстоят хуже, чем когда-либо. Однако это не ясно из предыдущих исследований, которые мы видели.

80%, 90% или 100%?

В 2014 году исследование, проведенное Industry Trust for Intellectual Property Awareness, показало, что 90% наиболее часто используемых пиратских сайтов фильмов и телепередач содержали вредоносное ПО или мошенничество с кредитными картами. Это больше, чем «восемь из десяти» сайтов в недавнем исследовании DCA.

Отчет Webroot компании OpenText Security Solutions, опубликованный в прошлом месяце, также показал, что 90% самых популярных нелегальных потоковых сайтов содержат опасный контент. И согласно FACT, то же исследование показало, что все проанализированные сайты содержали «вредоносный контент».

Основываясь на этих элементарных сравнениях, пиратские потоковые сайты ранее были намного более рискованными, чем в этом последнем отчете. Но это невозможно сказать наверняка, так как методологии и исследуемые сайты довольно сильно различаются.

ЕС не видел эпидемии вредоносного пиратства

Также стоит отметить, что есть исследования на эту тему, которые показывают совсем другую картину. Помимо тонких замечаний антивирусных экспертов, Ведомство интеллектуальной собственности ЕС также делает менее мрачный вывод.

В рамках подробного исследования, проведенного в нескольких странах ЕС, исследователи из ЕС изучили более 1000 доменов пиратских сайтов. Они обнаружили, что менее 10% этих сайтов связаны с вредоносным контентом, который включает в себя менее серьезное «потенциально нежелательное программное обеспечение». По мнению исследователей из ЕС, пиратские сайты не представляли особой проблемы.

«В настоящее время веб-сайты и потоковые сервисы, подозреваемые в нарушении авторских прав, обычно не считаются основными источниками

распространения вредоносных программ или иного нежелательного программного обеспечения», — говорится в исследовании.

Результаты отчета DCA «Нечестивый треугольник», если не сказать больше, совсем другие. Тем не менее, с различными методологиями и определениями «вредоносного» непросто сравнивать результаты.

В любом случае, приятно видеть, что группы правообладателей тратят так много времени и ресурсов на то, чтобы предупредить пиратов о вредоносном ПО. Помешает ли это людям посещать пиратские сайты, конечно, другой вопрос.

Возможно, основная цель отчета не в том, чтобы предупредить общественность в целом, а в том, чтобы предупредить власти о необходимости принять меры против пиратства. Это, по крайней мере частично, то, чего надеются достичь авторы, поскольку они призывают Министерство юстиции и Федеральную торговую комиссию принять меры.

«Как показывает этот отчет, злоумышленники используют бесплатный контент как «приманку», чтобы заманить пользователей в жертву. Поэтому жизненно важно, чтобы Министерство юстиции нацеливалось на вредоносные программы и пиратские сайты, которые настраивают пользователей на то, чтобы они стали жертвами программ-вымогателей и другого вредоносного программного обеспечения».

«Кроме того, FTC следует рассмотреть новые меры по предупреждению потребителей о рисках кибербезопасности, связанных с пиратством и появлением вредоносной рекламы на этих сайтах», — добавляется в отчете». ***(Ernesto Van der Sar. Piracy Advertising Researchers Fall Victim to Ransomware Attacks // TorrentFreak (https://torrentfreak.com/piracy-advertising-researchers-fall-victim-to-ransomware-attacks/). 18.09.2022).***

***

«Киберпреступники изучают новые способы проведения распределенных атак типа «отказ в обслуживании» (DDoS), чтобы сделать их более сложными для защиты и более эффективными для нарушения работы.

DDoS-атаки — это относительно простая, но эффективная форма кибератаки, при которой киберпреступники перегружают сервисы веб-трафиком, замедляя их работу или полностью отключая от сети, лишая других возможности их использовать. Атаки могут варьироваться от коротких кампаний, которые длятся несколько минут, до атак, растянутых на продолжительные периоды времени.

Эти атаки часто основаны на том, что зараженные вредоносным ПО компьютеры, серверы и устройства Интернета вещей подключаются к ботнету, который затем переполняет цель DDoS веб-трафиком.

Хотя DDoS-атаки просты по сравнению с другими вредоносными кибер-кампаниями, они могут привести к серьезным нарушениям. Крупные DDoS-кампании временно серьезно нарушили работу онлайн-сервисов, предприятий и даже онлайн-инфраструктур целых стран.

Преступники, стоящие за DDoS-атаками, которые часто сдают свои услуги в аренду для использования другими, продолжают находить новые способы сделать атаки более эффективными, согласно исследователям кибербезопасности из

Netscout, которые оценивают, что во всем мире было совершено более шести миллионов DDoS-атак. первая половина 2022 года.

Этот уровень DDoS-атак соответствует предыдущему шестимесячному периоду, но по мере того, как сети доставки контента и поставщики кибербезопасности лучше предотвращают DDoS-атаки, злоумышленники находят новые и инновационные способы усиления своих атак.

Исследователи подробно описывают два метода DDoS-атак, число которых увеличилось за последний год.

В первом новом типе атаки нацелен широкий спектр сервисов и/или устройств с меньшими порциями трафика по сравнению с обычным DDoS-инцидентом. Идея состоит в том, что несколько различных конвейеров цели перегружены без срабатывания пороговых значений, которые инициируют защиту от необычно высокого уровня трафика.

Многие системы защиты от DDoS-атак сосредоточены на отдельных IP-адресах, а не на целых подсетях, поэтому такие атаки часто остаются незамеченными.

Вторая новая атака заключается в том, что злоумышленники отправляют огромное количество фиктивных запросов поддоменов в попытке перегрузить службы прикладного уровня.

«Постоянно внедряя инновации и адаптируясь, злоумышленники разрабатывают новые, более эффективные векторы DDoS-атак или удваивают существующие эффективные методологии», — сказал Ричард Хаммел, руководитель отдела анализа угроз в Netscout.

Развиваются не только DDoS-атаки: киберпреступники также вкладывают ресурсы в расширение и добавление функций в ботнеты. Тайно заражая все больше машин вредоносными программами, киберпреступники могут использовать их для проведения более масштабных атак, и в отчете Netscout говорится, что ботнеты становятся все больше, как с точки зрения размера, так и с точки зрения возможностей.

«Без сомнения, ботнеты продолжают развиваться с пугающей скоростью. Их создатели не ограничены бюрократизмом, внутренними процессами, такими как Agile, или процессами утверждения. Их возможности расширяются с каждым годом, и их цели теперь варьируются от геймеров до геополитических врагов», — предупреждают исследователи.

«Все эти факторы заставляют организации защищаться от этих атак или рисковать массовыми сбоями в обслуживании и репутации», — добавили они.

Есть несколько шагов, которые организации могут предпринять, чтобы избежать сбоев в работе в результате DDoS-атак. Эти шаги включают в себя использование облачных хостинг-провайдеров, развертывание услуг IP-нагрузок для проверки пропускной способности и использование службы смягчения последствий DDoS». ***(Danny Palmer. Hackers are making DDoS attacks sneakier and harder to protect against // ZDNET (https://www.zdnet.com/article/hackers-are-making-ddos-attacks-sneakier-and-harder-to-protect-against/). 28.09.2022).***

***

«В фильмах хакеры обычно нажимают несколько клавиш и получают доступ ко всей сети за считанные секунды. Однако в реальном мире злоумышленники часто начинают с не более чем учетной записи пользователя низкого уровня, а затем работают над получением дополнительных привилегий, которые позволят им захватить сеть.

Одним из методов, который обычно используется для получения этих привилегий, является атака с передачей хеша.

За кулисами хэша пароля

Чтобы понять, как работает атака с передачей хеша, вы должны сначала понять, как используются хэши паролей.

Когда вы назначаете пароль системе, этот пароль фактически не сохраняется в системе. Вместо этого операционная система использует математическую формулу для вычисления хэша пароля. Хэш - это то, что хранится, а не фактический пароль.

Когда вы входите в систему, механизм аутентификации использует ту же математическую формулу для вычисления хэша введенного вами пароля и сравнивает его с сохраненным хэшем. Если два хэша совпадают, считается, что пароль правильный, и доступ предоставляется.

Важным выводом из этого является то, что с точки зрения системы хэш является паролем.

Злоумышленнику, который хочет получить доступ к системе, не всегда нужно знать пароль пользователя. Им просто нужно иметь доступ к хэшу пароля, который уже хранится в системе. С точки зрения хакера, иметь доступ к хэшу пароля — это, по сути, то же самое, что иметь доступ к паролю.

Хеширование паролей — широко используемый метод защиты паролей, но не все технологии хеширования паролей одинаковы. В этом посте описаны три основных типа методов хеширования паролей и способы изменения того, какой из них использует ваша Active Directory.

Что происходит, когда хэш скомпрометирован

Как отмечалось ранее, киберпреступники, которые хотят захватить сеть, обычно используют базовую учетную запись пользователя в качестве начальной точки входа. Они могут приобрести украденные учетные данные в даркнете, заразить пользователя вредоносной программой для кражи паролей или использовать множество других методов для получения пароля пользователя.

Как только хакер получает доступ к паролю низкоуровневого пользователя (фактический пароль, а не хеш), его следующим приоритетом является вход в систему под этим пользователем, а затем поиск способов повышения своих разрешений. Здесь в игру вступает атака pass-the-hash.

Распространенность передачи хэша в ОС Windows

Атака Pass-the-Hash может использоваться в различных системах, но чаще всего нацелена на системы Windows. Причина, по которой Windows является излюбленной целью, заключается в том, что системы Windows содержат хэши паролей для всех, кто когда-либо входил в эту систему. Не имеет значения, вошел ли пользователь в систему локально или использовал сеанс RDP. Их хеш все равно будет храниться в системе.

Когда хакер входит в систему, он ищет в системе любые хэши паролей, которые могут существовать, в надежде, что администратор вошел в систему в какой-то момент. Если хэши уровня администратора отсутствуют, хакер выполнит атаку с использованием хэш-распыления, в которой они используют украденные хэши паролей для входа на любую другую рабочую станцию и извлечения ее хэшей паролей.

В конце концов злоумышленник, скорее всего, обнаружит систему, содержащую хэш уровня администратора. Затем этот хэш можно использовать для получения доступа к контроллерам домена, серверам приложений, файловым серверам и другим конфиденциальным ресурсам.

Пять шагов для предотвращения атаки с передачей хеша в вашей сети

К сожалению, атаки с передачей хеша трудно обнаружить, поскольку эти атаки основаны на обычных механизмах аутентификации операционной системы. Таким образом, важно предпринять шаги, чтобы попытаться предотвратить успешные атаки с передачей хеша. Есть несколько вещей, которые вы можете сделать, чтобы уменьшить вероятность успешной атаки с передачей хеша.

Никогда не входите на рабочую станцию с привилегированной учетной записью

Прежде всего, вы никогда не должны входить на рабочую станцию, используя привилегированную учетную запись. Это включает сеансы RDP. Лучше всего настроить выделенные рабочие станции управления, защищенные от атак, и выполнять привилегированные операции исключительно с этих рабочих станций.

Включить Credential Guard в Защитнике

Windows Windows 10 и 11 включают инструмент под названием Credential Guard в Защитнике Windows. Этот инструмент, если он включен, использует виртуализацию на аппаратном уровне для запуска службы подсистемы локального органа безопасности в изолированной среде. Это простое действие делает систему гораздо более устойчивой к атакам с передачей хеша.

Применение принципа наименьшего доступа пользователей

Основная идея наименьшего доступа пользователей заключается в том, что у пользователей не должно быть никаких разрешений, кроме тех, которые необходимы им для выполнения своей работы. Хотя использование наименьшего пользовательского доступа не предотвратит атаку с передачей хэша, оно сведет к минимуму ущерб, если злоумышленнику удастся скомпрометировать одну или несколько учетных записей.

Используйте брандмауэры для блокировки ненужного трафика

Устройствам конечных пользователей, вероятно, потребуется доступ к контроллерам домена, файловым серверам и другим бизнес-системам. Тем не менее, одной рабочей станции достаточно редко требуется доступ к другой. Если вы можете использовать брандмауэры для блокировки трафика между рабочими станциями, то вы уменьшите способность злоумышленника совершать боковые движения, необходимые для успешной атаки с передачей хэша.

Используйте Specops Password Auditor для доступа к вашему паролю

Прежде чем злоумышленник сможет инициировать атаку с передачей хэша, ему требуется начальная точка входа. Обычно это происходит в виде украденных

учетных данных. Бесплатный инструмент под названием Specops Password Auditor может помочь вам определить учетные записи, подверженные риску, до того, как они будут скомпрометированы.

Specops Password Auditor не только проверяет, соответствуют ли пароли пользователей отраслевым стандартам для безопасных паролей, но также может сравнивать пароли пользователей со списком паролей, которые, как известно, были скомпрометированы. Таким образом, вы можете принудительно сменить пароль, прежде чем такую учетную запись можно будет использовать». ***(Pass-the-Hash Attacks and How to Prevent them in Windows Domains // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/pass-the-hash-attacks-and-how-to-prevent-them-in-windows-domains/). 27.09.2022).***

***

«Fast Company отключила свой веб-сайт после того, как его взломали, чтобы показывать истории и рассылать уведомления Apple News, содержащие непристойные и расистские комментарии. Сегодня хакер рассказал, как они якобы взломали сайт.

Сегодня на сайте представлено заявление компании, подтверждающее, что они были взломаны в воскресенье днем, а затем во вторник вечером произошел дополнительный взлом, который позволил злоумышленникам рассылать расистские уведомления на мобильные устройства через Apple News.

«Система управления контентом компании была взломана во вторник вечером. В результате примерно с разницей в минуту нашим подписчикам в Apple News были отправлены два непристойных и расистских push-уведомления», — говорится в заявлении на сайте Fast Company.

«Сообщения отвратительны и не соответствуют содержанию и духу Fast Company. Мы расследуем ситуацию и закрыли FastCompany.com до тех пор, пока ситуация не будет решена».

О непристойных уведомлениях Apple News быстро сообщили пользователи Twitter, в результате чего Apple News отключила канал Fast Company в службе новостей.

Хронология атаки

Первые признаки того, что Fast Company была взломана, появились в воскресенье днем, когда домашняя страница сайта начала заполняться статьями под заголовком «Взломал Винни Тройя. [отредактировано] язык мой [отредактировано]. Тракс был здесь»

Члены хакерского сообщества Breached и ныне закрытого RaidForums имеют давнюю вражду с исследователем безопасности Винни Тройей, где они обычно портят веб-сайты и совершают взломы, в которых обвиняют исследователя.

Fast Company отключила сайт на некоторое время, чтобы исправить искажение, но была снова взломана во вторник вечером около 20:00 по восточному поясному времени. На этот раз хакер рассылал уведомления Fast Company через Apple News, которые содержали такие же непристойные и расистские комментарии, как и дефейс веб-сайта.

Сегодня сайт снова был отключен, и на нем отображается заявление Fast Company, опубликованное выше.

Хакер рассказал, как взломал Fast Company

Судя по упоминанию «Винни Троя» в дефейсах, неудивительно, что участник хакерского форума Breached по имени «Тракс» делится информацией о том, как они якобы взломали веб-сайт Fast Company.

Злоумышленник утверждает, что им удалось взломать Fast Company после того, как они обнаружили экземпляр WordPress, используемый компанией для их веб-сайта.

Этот экземпляр WordPress якобы был защищен с помощью базовой HTTP-аутентификации, которая была обойдена. Затем злоумышленники говорят, что они получили доступ к WordPress CMS, используя очень простой пароль по умолчанию, который использовался для «десятков» учетных записей.

Оттуда, по их словам, им удалось украсть токены Auth0, ключи Apple News API и секреты Amazon SES.

Используя эти токены, они утверждают, что создали учетные записи администраторов в системах CMS, которые использовались для отправки уведомлений в Apple News.

BleepingComputer обычно не делится подробной информацией о том, как хакер получил доступ к сайту, но, поскольку Fast Company уже устраняет уязвимость, мы считаем, что эта информация может быть полезна другим администраторам веб-сайта.

Также следует отметить, что это утверждения злоумышленника, и BleepingComputer не имеет возможности самостоятельно проверить эту информацию.

BleepingComputer связался с Fast Company, чтобы подтвердить обоснованность этих утверждений, но наше электронное письмо было возвращено». ***(Lawrence Abrams. Hacker shares how they allegedly breached Fast Company's site // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hacker-shares-how-they-allegedly-breached-fast-company-s-site/). 28.09.2022).***

***

«Инструментарий постэксплуатации Brute Ratel был взломан и теперь бесплатно распространяется среди русскоязычных и англоязычных хакерских сообществ.

Для тех, кто не знаком с Brute Ratel C4 (BRC4), это набор инструментов для пост-эксплуатации, созданный Четаном Наяком, бывшим членом команды Mandiant и CrowdStrike.

Красные команды — это профессионалы в области кибербезопасности, чья работа состоит в том, чтобы попытаться взломать корпоративную сеть, чтобы выявить ее недостатки, в то время как члены синей команды пытаются защититься от этих атак.

После этих учений обе группы обсуждают, что было найдено для укрепления обороны и повышения безопасности.

Подобно Cobalt Strike, Brute Ratel — это набор инструментов, используемый членами красной команды для развертывания агентов, называемых барсуками, на скомпрометированных сетевых устройствах и их использования для удаленного выполнения команд и дальнейшего распространения по сети.

Brute Ratel взломан

За последние несколько лет взломанные версии Cobalt Strike настолько активно использовались злоумышленниками и бандами вымогателей, что программы безопасности легче обнаруживают их.

Из-за этого некоторые злоумышленники и банды вымогателей незаметно переходят на Brute Ratel для своих атак, якобы создавая поддельные американские компании для прохождения системы проверки лицензирования.

Однако ситуация вот-вот изменится, поскольку исследователь киберугроз Уилл Томас (также известный как BushidoToken) сообщил, что взломанная копия Brute Ratel в настоящее время широко циркулирует среди злоумышленников на хакерских онлайн-форумах.

«Теперь на самых популярных форумах по киберпреступности есть несколько сообщений, где тусуются брокеры данных, разработчики вредоносных программ, брокеры первоначального доступа и партнеры по вымогателям», — предупреждает Томас в новом отчете о взломанной версии Brute Ratel.

«Сюда входят BreachForums, CryptBB, RAMP, Exploit[.]in и Xss[.]is, а также различные группы Telegram и Discord».

После непродолжительного поиска на хакерских форумах XSS и Breached злоумышленники создали несколько тем, в которых они с середины сентября делились взломанной версией Brute Ratel C4 версии 1.2.2.

В прошлом разработчик Brute Ratel Четан Наяк сообщил BleepingComputer, что может отозвать лицензии у любых клиентов, злоупотребляющих Brute Ratel в злонамеренных целях.

Однако Наяк утверждает, что на VirusTotal была загружена невзломанная версия, которая затем была взломана «российской группой «Молекулы» для удаления проверки лицензии.

Независимо от того, как произошла утечка программного обеспечения, к сожалению, уже слишком поздно.

Томас сказал BleepingComputer, что взломанная версия работает и, похоже, не подделана, а это означает, что вскоре мы увидим широкое использование инструментария.

«Да, вам не нужно вводить лицензионный ключ, и ни я, ни мои коллеги из Curated Intel не выглядят подделанными», — пояснил Томас в разговоре с BleepingComputer.

На самом деле злоумышленники уже начали публиковать на хакерских форумах снимки экрана, на которых они тестируют инструментарий.

Что больше всего беспокоит Томаса, так это то, что Brute Ratel может генерировать шелл-код, который в настоящее время не так легко обнаружить программным обеспечением безопасности.

«Одним из наиболее важных аспектов инструмента BRC4 для многих экспертов по безопасности является его способность генерировать шелл-код,

который не обнаруживается многими продуктами EDR и AV», — пояснил Томас в своем отчете.

«Это расширенное окно уклонения от обнаружения может дать злоумышленникам достаточно времени, чтобы установить первоначальный доступ, начать боковое движение и добиться устойчивости в другом месте».

Томас рекомендует администраторам безопасности, Windows и сети просмотреть блог MdSec о Brute Ratel C4, чтобы узнать больше об обнаружении программного обеспечения в их сетях». ***(Lawrence Abrams. Hackers now sharing cracked Brute Ratel post-exploitation kit online // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-now-sharing-cracked-brute-ratel-post-exploitation-kit-online/). 28.09.2022).***

***

«Проміжний звіт про безпеку Check Point Software показує зростання кількості кібератак у світі на 42% із використанням програм-вимагачів як загрози номер один.

Середньорічний звіт за 2022 рік детально розглядає, як кібератаки посилилися та стали зброєю державного рівня з розквітом хактивізму в першій половині цього року з ключовими прогнозами щодо атак у Метавсесвіті та ланцюгу поставок.

Оскільки війна в Україні домінувала у заголовках ЗМІ, вплив цих подій на кіберпростір був драматичним за масштабом, оскільки кібератаки міцно закріпилися як зброя на державному рівні.

У середньорічному звіті про кібератаки за 2022 рік (2022 Cyber Attacks Mid-Year Report) докладно розглядається, як посилилися кібервійни, щоб стати невіддільною частиною підготовки та ведення справжніх військових дій з наслідками для урядів і підприємств у всьому світі, навіть для тих, які безпосередньо не беруть участі у агресії. Також досліджується взаємодія з кібервійною та пов’язаним із державою хактивізмом, щоб порушити повсякденне життя громадян і завдати їм реальної шкоди. Найкраще це ілюструється кібернападом на Коста-Ріка, який призвів до скалічення основних послуг, включаючи охорону здоров’я та внутрішні державні процеси. Там були припинені на деякий час медичні огляди та стягнення податків у цьому новому методі «вимагання в країні», що робить програми-вимагачі загрозою номер один у другій половині року.

Стосовно прогнозів на другу половину.

Фрагментування екосистеми програм-вимагачів буде подовжуватися. Хоча групи програм-вимагачів стали більш структурованими та працюють як звичайний бізнес із встановленими цілями, Check Point вважає, що надалі буде багато малих і середніх груп замість кількох великих груп. Як-от група Conti, засвоєний урок, оскільки їхній розмір і потужність привернули занадто багато уваги, що призвело до його падіння.

Більш різноманітними стануть ланцюжки зараження електронної пошти. Завдяки блокуванню Інтернет-макросів за замовчуванням у Microsoft Office, складніші сімейства зловмисних програм прискорять розробку нових ланцюжків зараження з різними типами файлів, які захищено паролем, щоб запобігти виявленню, у міру збільшення складних атак соціальної інженерії.

Хактивізм продовжуватиме розвиватися – групи активістів лише посилять узгоджування своїх атак з порядком денним обраної ними держави.

Посиляться кібератаки на децентралізовані блокчейн-мережі з очікуваними першими атаками в Metaverse. З великими інцидентами, пов’язаними з платформами блокчейнів, такими як уразливість Rarible або ApeCoin Airdrop, ми очікуємо, що хакери продовжуватимуть намагатися зламати та викрадати криптоактиви. Крім того, ми побачимо початкові атаки в Metaverse, які використовуватимуть вразливості смарт-контрактів.

Теоретичний потенціал кіберсервісу для серйозного підриву в громадянському суспільстві став реальним у 2022 році, і звіт тільки підкріплює ці тенденції та інші аспекти ландшафту загроз, що розвиваються». ***(Олександр Савушкін. 2022 Cyber Attacks Report: зріст на 42%, хактивізм та атаки у Метавсесвіті // Компьютерное Обозрение (https://ko.com.ua/2022_cyber_attacks_report_zrist_na_42_haktivizm_ta_ataki_u_metavsesviti_142206). 28.09.2022).***

***

«Використання кіберзлочинцями дипфейків, фальсифікованих медіа з високою довірою продовжує зростати. Ми зібрали добірку рекомендацій, як можна протидіяти технології дипфейків.

Наразі поширені дипфейк-атаки використовують сфабриковані зображення знаменитостей, зазначається в дослідженні Trend Micro. Щоб спонукати жертв натискати на рекламу, купувати шахрайські продукти або брати участь у різних видах інвестицій. Але тепер також є випадки, коли жертв обманювали за допомогою відеодзвінків, де зловмисники видавали себе за іншу осіб.

Все необхідне для використання дипфейків у кібератаках у вигляді інструментів і ресурсів зображень доступне як у відкритому інтернеті, так і на секретних форумах.

Нижче ми зібрали найбільш поширені зараз різновиди атак технології дипфейків, а також рекомендації, як їм протидіяти.

Різновиди атак технології дипфейків

Шахрайство у месенджерах. Видача себе за керуючого коштами та дзвінки з приводу грошового переказу були популярною аферою протягом багатьох років, і тепер злочинці можуть використовувати дипфейки у відеодзвінках. Наприклад, вони можуть видати себе за когось і зв'язатися зі своїми друзями та сім'єю, щоб запросити грошовий переказ або запросити просте поповнення балансу свого телефону.

Ведення рахунків. Злочинці можуть використовувати дипфейки для обходу служб перевірки особи та створення облікових записів у банках та фінансових установах, можливо навіть у державних службах, від імені інших людей, використовуючи копії вкрадених документів, що засвідчують особу. Такі облікові записи згодом можуть бути використані для відмивання грошей та інших зловмисних дій.

Зламування облікових записів. Злочинці можуть заволодіти обліковими записами, які потребують ідентифікації за допомогою відеодзвінків. Вони можуть захопити фінансовий рахунок та просто зняти чи переказати кошти. Деякі фінансові

установи потребують онлайн-відеоперевірки, щоб включити певні функції у додатках онлайн-банкінгу. Очевидно, такі перевірки також можуть стати метою дипфейкових атак.

Шантаж. Використовуючи дипфейкові відео, зловмисники можуть проводити більш потужні здирства та інші атаки, пов'язані з вимаганням. Вони навіть можуть підкидати підроблені докази, створені за допомогою технологій дипфейків.

Кампанії з дезінформації. Відео з дипфейками також створюють ефективніші кампанії з дезінформації та можуть використовуватися для маніпулювання громадською думкою. Деякі атаки, такі як схеми накачування та скидання, ґрунтуються на повідомленнях від відомих осіб. Тепер ці повідомлення можна створювати за допомогою технології дипфейків. Ці схеми, безумовно, можуть мати фінансові, політичні та навіть репутаційні наслідки.

Шахрайство із службою технічної підтримки. Суб'єкти дипфейків можуть використовувати підроблені посвідчення особи, щоб за допомогою соціальної інженерії змусити користувачів, які нічого не підозрюють, ділитися обліковими даними для оплати або отримати доступ до IT-активів.

Атаки соціальної інженерії. Зловмисники можуть використовувати дипфейки для маніпулювання друзями, сім'ями або колегами.

Зламування пристроїв Інтернету речей (IoT). Пристрої, які використовують розпізнавання голосу або особи, такі як Alexa від Amazon і багато інших брендів смартфонів, будуть у списку цілей зловмисників, які займаються дипфейками.

Як можна протидіяти дипфейкам

Підхід до багатофакторної аутентифікації повинен бути стандартним для будь-якої аутентифікації конфіденційних або важливих облікових записів.

Організації повинні аутентифікувати користувача за трьома основними факторами: щось, що є у користувача, щось, що користувач знає, і щось, чим є користувач. Переконайтеся, що це «щось» вибрано з розумом.

Навчання персоналу за принципом «знай свого клієнта» (KYC) особливо важливе для фінансових організацій. Технологія дипфейків не є ідеальною, і є певні сигнали, на які слід звернути увагу персоналу організації.

Користувачі соціальних мереж повинні мінімізувати показ високоякісних особистих зображень.

Для перевірки конфіденційних облікових записів (наприклад, банківських або корпоративних профілів) користувачі повинні надавати перевагу використанню біометричних шаблонів, які менш доступні для громадськості. Це, наприклад, сканування райдужної оболонки ока та відбитків пальців.

Для розв'язання проблеми у ширшому масштабі необхідні значні зміни у політиці задля скасування використання поточних та раніше розкритих біометричних даних. Вони також повинні враховувати поточний стан кіберзлочинної діяльності та готуватися до майбутнього». ***(Вадим Добровольський. Кіберзлочинці дедалі частіше використовують дипфейки. Як цьому протидіяти // speka.media (https://speka.media/yak-protidiyati-dipfejkam-v56gnp). 28.09.2022).***

***

«Lazarus Group, северокорейская продвинутая группировка постоянных угроз, недавно атаковала энергетические компании в Канаде, США и Японии, чтобы установить долгосрочный доступ к сетям жертв для проведения шпионских операций путем развертывания специально созданных вредоносных имплантатов.

Последняя кампания, отслеживаемая исследователями Cisco Talos, показала, что злоумышленники использовали уязвимости в VMware Horizon, чтобы первоначально закрепиться в целевых организациях, после чего было развернуто созданное группой специально разработанное вредоносное ПО VSingle, YamaBot и ранее неизвестное вредоносное ПО, получившее название MagicRAT.

Исследователи говорят, что кампания направлена на установление долгосрочного доступа к сетям жертв, чтобы выкачивать интеллектуальную собственность, принадлежащую неназванным энергетическим компаниям.

Вредоносная активность была обнаружена в период с февраля по июль 2022 года. Злоумышленники использовали уязвимость Log4Shell на общедоступных серверах VMware Horizon в нескольких кампаниях в качестве начального вектора атаки…

Детали кампании

RAT, идентифицированные исследователями, VSingle и YamaBot, разрабатываются и распространяются Lazarus. Японский CERT опубликовал подробности о них и приписал кампании Lazarus.

Исследователи говорят, что они наблюдали несколько атак, нацеленных на несколько жертв, и что два конкретных случая атаки являются наиболее «представителями сценариев, использованных Lazarus в этой кампании».

Первый пример — это использование имплантата VSingle, а второй — развертывание MagicRAT вместе с VSingle. Следует отметить третий набор вторжений — использование третьего имплантата, известного как YamaBot.

Используя уязвимость Log4Shell на общедоступных серверах VMWare Horizon в качестве начального вектора атаки, исследователи Cisco Talos говорят, что за компрометацией следует ряд действий, направленных на то, чтобы закрепиться в системах, прежде чем злоумышленники разместят дополнительное вредоносное ПО и переместятся в горизонтальном направлении. сеть.

В ходе расследования они обнаружили два разных плацдарма. В первом они использовали abused node.exe, который поставляется с VMware для выполнения node.exeсценария oneliner, который помогает открыть «интерактивную обратную оболочку, которую злоумышленники могут использовать для выполнения произвольных команд на зараженной конечной точке входа».

Другой пример — использование уязвимостей в VMWare для запуска пользовательских сценариев PowerShell на зараженной конечной точке через VMWare ws_ConnectionServer.exe.

«Поскольку VMware Horizon запускается с правами администратора, злоумышленнику не нужно беспокоиться о повышении своих привилегий. После установки интерактивной оболочки злоумышленники проводят предварительную

разведку на конечной точке, чтобы получить информацию о сети и списки каталогов», — исследователи. сказать.

На следующем этапе злоумышленники деактивируют компоненты Защитника Windows с помощью изменений ключа реестра, команд WMIC и команд PowerShell.

После успешного отключения AV в системе с помощью обратной оболочки злоумышленники могут развернуть вредоносный имплант VSingle.

Весь процесс развертывания включает в себя загрузку законной утилиты WinRAR из удаленного места, контролируемого злоумышленниками, вместе с дополнительной полезной нагрузкой.

Дополнительная полезная нагрузка, загружаемая на конечную точку, распаковывается и состоит из «исполняемого вредоносного файла VSingle, который при необходимости переименовывается, а затем сохраняется на конечной точке путем создания службы автоматического запуска».

Расследование Cisco Talos привело к обнаружению команд, переданных злоумышленниками бэкдору VSingle для выполнения различных действий, таких как разведка, эксфильтрация и ручное бэкдорирование.

В ходе одной из попыток вторжения исследователь обнаружил, что злоумышленники изначально развернули VSingle на конечной точке, но позже, когда образец был обнаружен, он рисковал потерять доступ к предприятию. В этом случае злоумышленники развернули другой вариант VSingle для поддержания постоянного доступа, прежде чем, наконец, перейти к имплантату YamaBot.

Созданное на заказ семейство вредоносных программ на основе GoLang YamaBot использует HTTP для связи со своими серверами управления и контроля и начинает с отправки предварительной системной информации о зараженной конечной точке на C2: имя компьютера, имя пользователя и MAC-адрес.

Этот имплантат имеет стандартные возможности RAT, такие как список файлов и каталогов, и он может отправлять информацию о процессе на C2, загружать файлы из удаленных мест, выполнять произвольные команды на конечных точках и удалять себя.

Открытие MagicRAT

В другой сети-жертве исследователи Cisco Talos наблюдали аналогичную цепочку событий: первоначальная разведка, затем отключение антивирусного программного обеспечения и развертывание имплантата.

Они также наблюдали боковое перемещение в другие конечные точки предприятия. «Однако уникальность этого вторжения заключается в том, что мы наблюдали развертывание довольно нового имплантата за три дня до того, как злоумышленники развернули VSingle на зараженных системах», — говорят исследователи.

В дальнейших боковых перемещениях после первоначального доступа злоумышленники провели ограниченную разведку конечной точки и развернули два разных семейства вредоносных программ, MagicRAT и VSingle, для поддержания скрытого доступа.

«Затем злоумышленники начали проводить исследования, связанные с Active Directory, чтобы определить потенциальные конечные точки для бокового перемещения», — говорят исследователи. «После получения списка компьютеров и

пользователей злоумышленники будут вручную пинговать определенные конечные точки в списке, чтобы проверить, доступны ли они».

Исследователи наблюдали за развертыванием инструментов impacket на определенных конечных точках для бокового перемещения и создания интерактивной оболочки, что выполнялось вручную оператором-человеком.

«Пытаясь установить интерактивные сеансы удаленной консоли, мы видим, как операторы допускают ошибки в командах», — говорят исследователи.

Эти злоумышленники не торопятся исследовать зараженную машину, и всякий раз, когда они находят интересующий файл, они помещают его в архив.rar для эксфильтрации с помощью одного из специально разработанных имплантатов, работающих в системе.

Цепочки заражения остались прежними, но некоторые из других ключевых вариаций, наблюдаемых исследователями, включают необязательные действия, проводимые группой APT при различных попытках вторжения:

Сбор учетных данных с использованием таких инструментов, как Mimikatz и Procdump;

Прокси-инструменты для настройки SOCKS-прокси;

Инструменты обратного туннелирования, такие как plink PuTTY». ***(Prajeet Nair. Latest Lazarus Campaign Targets Energy Companies // Information Security Media Group, Corp. (https://www.govinfosecurity.com/latest-lazarus-campaign-targets-energy-companies-a-20039). 10.09.2022).***

***

«Было замечено, что спонсируемая российским государством хакерская группа, известная как Sandworm, маскируется под поставщиков телекоммуникационных услуг, чтобы атаковать украинские организации вредоносным ПО.

Песчаный червь — поддерживаемая государством угроза, которую правительство США считает частью российской службы внешней военной разведки ГРУ.

Считается, что хакерская группа APT стояла за многочисленными атаками в этом году, включая атаку на украинскую энергетическую инфраструктуру и развертывание устойчивой бот-сети под названием Cyclops Blink.

Начиная с августа 2022 года исследователи из Recorded Future наблюдали рост инфраструктуры управления и контроля (C2) Sandworm, которая использует динамические домены DNS, маскирующиеся под украинских поставщиков телекоммуникационных услуг.

Недавние кампании направлены на развертывание обычных вредоносных программ, таких как Colibri Loader и Warzone RAT (троян удаленного доступа), в критически важных украинских системах.

Хотя Sandworm значительно обновила свою инфраструктуру C2, она делала это постепенно, поэтому исторические данные из отчетов CERT-UA позволили Recorded Future с полной уверенностью связать текущие операции с субъектом угрозы.

Одним из примеров является домен «datagroup[.]ddns[.]net», обнаруженный CERT-UA в июне 2022 года и маскирующийся под онлайн-портал украинского оператора связи «Датагруп».

Еще одним поддельным украинским провайдером телекоммуникационных услуг является «Киевстар», для которого Sandworm использует фасады «киевстар[.]дднс[.]нет» и «киевстар[.]онлайн».

Более свежий случай касается «ett[.]ddns[.]net» и «ett[.]hopto[.]org», что, скорее всего, является попыткой имитации онлайн-платформы ООО «ЕвроТрансТелеком», другого украинского оператора связи.

Многие из этих доменов разрешаются в новые IP-адреса, но в некоторых случаях есть совпадения с прошлыми кампаниями Sandworm, начатыми еще в мае 2022 года.

Атака начинается с заманивания жертв посетить домены, как правило, через электронные письма, отправленные с этих доменов, чтобы создать впечатление, что отправитель является украинским оператором связи.

На этих сайтах используется украинский язык, а представленные темы касаются боевых действий, сообщений администрации, отчетов и т. д.

Самая распространенная веб-страница, просматриваемая Recorded Future, содержит текст «ОДЕСЬКА ОБЛАСНА ВІЙСЬКОВА АДМІНІСТРАЦІЯ»…

HTML-код веб-страницы содержит файл ISO в кодировке base64, который автоматически загружается при посещении веб-сайта с использованием метода контрабанды HTML.

Примечательно, что контрабанда HTML используется несколькими спонсируемыми российским государством хакерскими группами, недавним примером которой является APT29.

Полезная нагрузка, содержащаяся в файле образа, — это Warzone RAT, вредоносное ПО, созданное в 2018 году и достигшее пика популярности в 2019 году. Sandworm использует его для замены DarkCrystal RAT, который они развернули в предыдущие месяцы.

Возможно, российские хакеры хотят затруднить отслеживание и атрибуцию для аналитиков безопасности, используя широкодоступное вредоносное ПО и надеясь, что их следы «затеряются в шуме».

Вредоносное ПО WarZone RAT может быть старым, но оно по-прежнему предлагает мощные функции, такие как обход UAC, скрытый удаленный рабочий стол, кража файлов cookie и паролей, живой кейлоггер, файловые операции, обратный прокси-сервер, удаленная оболочка (CMD) и управление процессами». ***(Bill Toulas. Russian Sandworm hackers pose as Ukrainian telcos to drop malware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-pose-as-ukrainian-telcos-to-drop-malware/). 19.09.2022).***

***

«Согласно исследованию, проведенному исследователями из Технологического института Джорджии, около 25 000 веб-сайтов WordPress содержат вредоносные плагины WordPress.

94% из 47 337 вредоносных плагинов, установленных в период с 2012 по 2021 год, были активны на 24 931 уникальном веб-сайте WordPress, на каждом из которых было по два или более вредоносных плагина. Согласно исследованию, установка вредоносных плагинов со временем увеличилась, достигнув пика в марте 2020 года.

Исследователи обвинили «неявное доверие к большому количеству кода с неограниченным доступом к веб-серверу» в ужасающей ситуации с безопасностью.

Используя исследовательскую структуру YODA, выводы исследования Mistrust Plugins You Must были основаны на анализе кода, поведения и метаданных 400 000 анонимных резервных копий веб-сайтов из CodeGuard.

Владельцы веб-сайтов покупали зараженные плагины WordPress на законных торговых площадках.

8-летнее исследование количественно оценило стоимость вредоносных и пиратских плагинов WordPress на законных торговых площадках.

Было обнаружено, что популярные и законные торговые площадки, такие как ThemeForest, CodeCanyon и Easy Digital Downloads, были источниками 3685 вредоносных плагинов WordPress.

Исследователи обнаружили, что владельцы веб-сайтов потратили 41 500 долларов на зараженные плагины, продаваемые на платных сайтах с плагинами, а атаки после эксплуатации оцениваются в 834 000 долларов. Точно так же пиратские плагины обходятся разработчикам плагинов WordPress в $228 000 упущенной выгоды.

По словам исследователей, хотя рынок систем управления контентом приносил более 1 миллиарда долларов в год, мало что было сделано для обеспечения безопасности клиентов.

Впоследствии пользователям приходилось полагаться на простые показатели, такие как популярность, рейтинги и отзывы, чтобы определить, безопасен ли плагин WordPress. Злоумышленники использовали это скрытое доверие для распространения вредоносных плагинов WordPress среди ничего не подозревающих пользователей.

Кроме того, они приобретали кодовые базы популярных бесплатных плагинов, внедряли вредоносный код и ждали, пока автоматические обновления заразят веб-сайты, использующие бесплатный плагин.

«Хотя владельцы веб-сайтов доверяли экосистеме плагинов и потратили в общей сложности 7,3 миллиона долларов только на плагины в нашем наборе данных, мы обнаружили, что это доверие часто нарушается для получения денежной выгоды злоумышленниками», — заявили исследователи.

Кроме того, разработчики вредоносных программ подделывали добросовестных авторов подключаемых модулей для распространения пиратских зараженных подключаемых модулей. Исследователи обнаружили 1354 пиратских плагина, используемых в кампаниях по вредоносной рекламе.

Киберпреступники пиратили версии платных плагинов, которые предлагали пробную версию, внедряя «нулевые» плагины, содержащие вредоносный код. Исследование показало, что 97% обнуленных плагинов с таких торговых площадок, как vestathemes[.]com (96%), wplocker[.]com (98%), theme123[.]net (100%) и themelot[.]net (100%). %) продемонстрировали вредоносное поведение. Владельцы веб-сайтов получили не менее 6 223 вредоносных плагинов с обнуленных торговых площадок.

«Проверка PITA также проблематична, потому что существуют тысячи таких PITA без четкого происхождения, результатов тестирования или диаграмм потоков данных», — сказал Сунил Ю, директор по информационной безопасности в JupiterOne. «Команды безопасности используют рудиментарные подходы, чаще всего бегло рассматривая то, что я называю тремя Ps: популярность, цель и разрешения».

Вредоносные плагины WordPress могут перекрестно заражать и запускать атаки ATO

Исследователи обнаружили, что вредоносные плагины WordPress атаковали другие ресурсы на веб-серверах с установленным WordPress. Они перекрестно заражали другие плагины и использовали существующие уязвимости для сохранения устойчивости. Не менее 40 000 зараженных плагинов были скомпрометированы после развертывания.

Кроме того, исследователи обнаружили 10 000 веб-оболочек и методов обфускации кода для сокрытия вредоносного поведения.

Такие эксплойты могут привести к полному захвату веб-сайтов киберпреступниками и другим возможным атакам.

К сожалению, владельцы веб-сайтов не избавили свои веб-сайты от вредоносных плагинов WordPress, что позволило злоумышленникам сохранить настойчивость. Согласно исследованию, только 10% владельцев веб-сайтов пытались очистить свои веб-сайты, а 12% защищенных веб-сайтов повторно заражались.

Кроме того, исследование показало, что хотя некоторые вредоносные плагины больше не доступны на рынке, они все еще существуют на взломанных веб-сайтах.

«WordPress — одна из самых популярных в мире CMS, которая позволяет любому создавать динамические веб-сайты, — сказал Джон Бамбенек, главный охотник за угрозами в Netenrich. «Проблема в том, что он позволяет любому создавать динамические веб-сайты.

«Большинство людей используют свои веб-сайты в режиме «установил и забыл», что означает, что они понятия не имеют, были ли внесены какие-либо изменения, пока веб-сайт «работает правильно».

Исследователи заявили, что владельцы веб-сайтов должны привлекать опытных разработчиков и группы безопасности для удаления вредоносных плагинов WordPress из сред после разработки.

По словам Кори Клайна, старшего консультанта по кибербезопасности в nVisium, организациям также следует проверять плагины WordPress перед их развертыванием: «Это упрощается благодаря тому, что все плагины WordPress написаны на PHP, и их исходный код может быть проверен по желанию любым

пользователем. хочет сделать это». ***(Alicia Hope. Over 47,000 Malicious WordPress Plugins Are Active on Nearly 25,000 Websites // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/over-47000-malicious-wordpress-plugins-are-active-on-nearly-25000-websites/). 09.09.2022).***

***

«В последнем отчете о ландшафте угроз Агентства ЕС по кибербезопасности так называемые ботнеты названы наиболее часто обнаруживаемой категорией вредоносных программ в корпоративных средах. Взаимосвязанная экосистема Интернета вещей и Индустрии 4.0 особенно уязвима и представляет собой идеальную питательную среду для кибератак, осуществляемых ботнетами.

Что такое ботнеты? Как используются ботнеты?

Киберпреступники используют так называемые «ботнеты» для доступа к данным, хранящимся на предприятиях, удаленно и без обнаружения, для развертывания программ-вымогателей на серверах компаний или для временного отключения ИТ-инфраструктуры предприятия или его веб-служб, например, с помощью так называемого распределенного отказа в обслуживании. Сервисные (DDOS) атаки.

Ботнет состоит из почти бесконечного количества зараженных бот-программами устройств, соединенных друг с другом. Они служат киберпреступной инфраструктурой для крупномасштабных кибератак. Ботнеты используются не только создавшими их киберпреступниками, но и предоставляются третьим лицам за плату (ботнеты как услуга).

Как предприятия могут смягчить последствия атаки ботнета?

Если атака ботнета приводит к утечке личных данных, предприятия сталкиваются с различными обязательствами. Например:

Предприятия в Европе должны уведомить компетентные органы по защите данных без неоправданной задержки и в любом случае в течение 72 часов после того, как стало известно о нарушении.

Компании в США должны оценить конкретные требования к отчетности об утечке данных в своем штате, поскольку во всех штатах приняты правила уведомления отдельных лиц и/или регулирующих органов, а также более подробно ознакомиться с последним руководством Федеральной торговой комиссии от мая 2022 года. Последнее предусматривает, что нераскрытие информации об утечке данных затронутым сторонам может привести к нарушению Закона о Федеральной торговой комиссии и может привести к принудительным действиям со стороны Федеральной торговой комиссии.

В разных юрисдикциях Азиатско-Тихоокеанского региона и остального мира могут действовать различные законы об уведомлении о нарушениях, даже в странах, где защита данных и регулирование кибербезопасности в прошлом не были в центре внимания законодателей и регулирующих органов.

Также может применяться дополнительное отраслевое законодательство по безопасности ИТ. Компании в определенных секторах критической инфраструктуры должны выполнять обязательства по отчетности в соответствии с Директивой ЕС по

NIS и/или Законом США об отчетах о кибер-инцидентах для критической инфраструктуры (CIRCIA).

Хотя невыполнение этих требований к уведомлению может привести к принудительным мерам со стороны компетентного органа по защите данных, правоохранительные органы неоднократно подчеркивают необходимость того, чтобы предприятия сотрудничали с правоохранительными органами и предъявляли уголовные обвинения для эффективной борьбы с киберпреступностью. Например, в своем последнем отчете о состоянии киберпреступности в Германии Федеральное полицейское управление подчеркивает важность помощи частного бизнеса в уничтожении ботнета Emotet в 2021 году.

И виновник ботнета, и жертва?

Учитывая экономические потери, вызванные утечкой данных для предприятий, борьба с киберпреступниками служит внутренним коммерческим интересам каждой компании. Успешное уголовное расследование может не только привести к судебному преследованию бот-мастера, использующего ботнет, но и помочь в борьбе с поставщиками ботнетов как услуг.

Однако любая мера по оказанию помощи правоохранительным органам представляет собой раскрытие информации, которая может иметь отношение к другим регулирующим органам и заявителям в судебных разбирательствах, в частности, если оспаривается целесообразность технических и организационных мер кибербезопасности. Таким образом, жертва может быстро стать преступником, в зависимости от планов соответствующих органов. Поэтому каждый шаг сотрудничества должен быть тщательно взвешен с учетом регуляторных и судебных рисков, и, по возможности, должны быть приняты меры для обеспечения конфиденциальности сообщений.

Следует также учитывать, что правоохранительные органы могут потенциально принять решение в ходе установления фактов властями провести обыск в центре обработки данных предприятия или других объектах, если компания не будет сотрудничать. Это может нанести ущерб репутации и вызвать тревогу у других регулирующих органов, которые могут предположить, что бизнесу не хватает надежной политики после нарушения, и, таким образом, более тщательно изучить его технические и организационные меры. Недостатки в этом отношении привели к большим штрафам, и мы наблюдаем значительный поток массовых претензий (от затронутых клиентов или даже сотрудников) против компаний, пострадавших от утечки данных.

Депутаты о правонарушении

По мере роста числа атак ботнетов регулирующие органы Европы и США призывают к расширению законодательства о киберпреступности, что может повлиять на будущую оценку рисков предприятий после атаки ботнета.

В Германии Федеральный совет в третий раз с 2016 года внес законопроект о цифровом вторжении с целью расширения уголовной ответственности за создание ботнетов.

В США в июне 2021 года в Сенат был внесен Закон о предотвращении международной киберпреступности, который укрепит полномочия Министерства юстиции в отношении закрытия бот-сетей.

Предприятиям рекомендуется тщательно учитывать киберриски, такие как атаки бот-сетей, и принимать меры как для соблюдения все более строгих требований к защите данных, так и для защиты от рисков (уголовной) ответственности». ***(Botnet attacks and how businesses should respond // Freshfields Bruckhaus Deringer LLP (https://technologyquotient.freshfields.com/post/102hx51/botnet-attacks-and-how-businesses-should-respond). 19.06.2022).***

***

«У дешевого интернета и доступных облачных технологий есть и обратная сторона — ботнеты. Ранее киберпреступники создавали их на основе локальных серверов. Однако с развитием облачных технологий и Интернета вещей количество устройств, виртуальных машин и физических серверов — потенциальных элементов ботнетов — выросло в геометрической прогрессии.

Эксперты считают, что развитие бессерверных технологий еще больше упростит создание ботнетов. Вот как мы можем противостоять этому.

Начнем с теории. Какое оборудование и технологии можно использовать для проведения атак? Вот несколько основных вариантов:

Физические серверы — самый неудобный и дорогой вариант для злоумышленника. Однако, когда злоумышленники нацелены на физические серверы, достаточно заразить инфраструктуру и заставить ее атаковать случайные цели в ботнете, чтобы заблокировать его на разных уровнях стека.

Виртуальные машины — любимое оружие владельцев ботнетов. Облачные платформы постоянно развиваются, чтобы быстрее создавать и доставлять виртуальные экземпляры клиентам. Это также играет на руку злоумышленникам: они получают быстрый доступ к большому пулу дешевых ресурсов.

Устройства IoT — частая жертва создателей ботнетов. Эти сети устройств, подключенных к Интернету вещей (обычно маршрутизаторы), могут быть заражены вредоносными программами и использоваться в атаках.

Еще одна технология, которую потенциально могут использовать киберпреступники, — бессерверные вычисления. Предполагается, что с развитием облачных сервисов, таких как «Функция как услуга» (FaaS), владелец ботнета вообще не будет нуждаться в какой-либо инфраструктуре, имея возможность использовать блоки без сохранения состояния, которые выполняют код по расписанию, а затем отключаются. В этом случае каждый триггер создает новый экземпляр одной и той же функции. К счастью, случаев использования бессерверных вычислений для ботнетов, кроме контролируемых экспериментов, пока не зафиксировано.

Хотя злонамеренное использование бессерверных технологий все еще остается теорией, давайте рассмотрим более традиционную инфраструктуру — физическую или виртуальную. В большинстве случаев злоумышленники заражают такую инфраструктуру, используя массовые уязвимости. Работает это следующим образом: при обнаружении уязвимости в маршрутизаторах определенной марки или модели злоумышленники сканируют сети и в больших количествах устанавливают

на маршрутизаторы вредоносное ПО для осуществления атак с них. То же самое верно для физических серверов и виртуальных машин.

Киберпреступники запускают бота на каждом узле зараженной инфраструктуры. Этот небольшой скрипт автоматически выполняет заданную функцию — DDoS-атаку. Количество таких атак растет с каждым годом, увеличивается объем входящего трафика и, как следствие, увеличивается нагрузка на периметр безопасности.

Как должны действовать облачные провайдеры в этих новых условиях? Конечно, вы можете просто продолжать увеличивать мощность центров фильтрации, чтобы они поглощали растущий объем трафика. Однако это приведет к новым трудностям: во-первых, это дорого, а во-вторых, эти центры потребуют регулярного обслуживания, замены оборудования и прочего. Вот почему различные облачные и хостинговые провайдеры, желающие блокировать вредоносный трафик и оставлять законные запросы, стараются максимально перераспределить нагрузку. CDN идеально подходит для распределения нагрузки. Вот как это работает.

Центр очистки Gcore Protection состоит из трех уровней:

Защита от DDOS — этот уровень включает в себя решения для защиты от объемных атак L3/L4.

Защита от ботов — это набор алгоритмов очистки трафика, уже проникшего за периметр.

WAF — это брандмауэр для защиты веб-приложений от взлома и доступа к конфиденциальным данным.

Эта многоуровневая система безопасности позволяет нам анализировать все запросы. Если он видит, что есть много запросов на один URL с одного IP, сессия помечается и блокируется. Система автоматически реагирует на превышение требований, так как отслеживает среднюю нагрузку на ресурсы и далее самостоятельно определяет нормальные и аномальные значения. Таким образом, он пропускает легитимный трафик, но блокирует такие объемные атаки, как UDP/ICMP-флуд, усиление, SYN-ACK и RST-SYN-флуд на первом уровне защиты. Еще интереснее ситуация становится с другим вектором атаки — HTTP-флудом.

Второй уровень центра очистки — Bot Protection — отвечает за защиту от HTTP-флуда. С этими типами атак нужно быть более осторожными, чтобы не заблокировать подозрительные IP-адреса без дополнительной проверки, так как за ними, за NAT, стоят как легитимные посетители, так и пользователи, чьи компьютеры заражены.

Чтобы этого не произошло, мы используем многоэтапную аналитику:

Поведенческий анализ. Проверка количества и частоты запросов.

JS вызов/капча. Прежде чем решить, что мы имеем дело с ботом, мы отправляем запрос на проверку с помощью JS Challenge/Captcha.

Первый метод — JS Challenge — предполагает отправку кода JavaScript клиенту с конкретной задачей. Если пользователь легитимен и, в отличие от обычного бота, использует браузер с поддержкой JavaScript, он пройдет тест, даже не заметив этого — ему не придется метить светофоры и велосипеды.

Второй метод — JS Captcha — менее интеллектуален, но более надежен. После выполнения вызова клиент временно включается в список проверенных IP-адресов.

Помимо прочего, во время теста мы узнаем информацию, которая полезна для защиты от ботов, и которую мы используем в дальнейшем (например, версию браузера).

Анализ заголовков HTTP. Сравнение заголовков и результатов JS Challenge.

Анализ сеанса TLS с использованием хэша JA3. Хэш JA3 — эффективный способ анализа сеанса. Каждый хэш состоит из нескольких значений, позволяющих определить клиента. Поскольку он создается с помощью специальной хэш-функции на основе информации, полученной в рамках пакета TLS Hello, каждую версию браузера и каждого клиента можно идентифицировать, сравнивая полученный хэш с тем, который хранится в базе данных центра фильтрации.

Когда центр фильтрации обнаруживает внутри TLS Hello хэш, которого нет в базе данных или который явно нелегитимен — например, хеш JA3 получен от curl с надписью «Internet Explorer» в User Agent — центр блокирует его или запускает проверку.

Все эти этапы тестирования наглядно демонстрируют, как работает защита от ботов на высоком уровне. Но что происходит внутри, на более низком уровне?

В случае серьезных атак активируется интеграция с eBPF, которая блокирует атаки на L3—L4. Таким образом, мы также снижаем риск перегрузки центра фильтрации.

Комбинированное использование технологий низкоуровневого анализа вместе с алгоритмическими методами сверху снижает вероятность блокирования легитимного трафика, даже если и вредоносный, и легитимный трафик исходят с одного и того же IP-адреса. Наш показатель ложных срабатываний составляет менее 0,01%.

Почему мы решили использовать eBPF? Поскольку это монолит, встроенный в ядро — по сравнению с тем, что использовался раньше (dpdk), некоторые проблемы решаются проще, а иногда и полностью устранены. Например, в отличие от dpdk, eBPF можно использовать на одном сетевом интерфейсе вместе с другой ролью. Поэтому в дальнейшем мы планируем активнее использовать его на узлах CDN, работающих на мощных процессорах Intel® Xeon® Scalable 3-го поколения.

У Gcore большая сеть доставки контента — ее общая пропускная способность составляет около 100 ТБ трафика в секунду, но при этом дуплексный канал используется на 85% исходящего трафика (клиенты получают контент), а входящий канал используется недостаточно. Благодаря интеграции CDN и eBPF мы планируем подключить эти мощности к очистке трафика, оставаясь максимально близко к клиенту.

Пользователи Gcore имеют комплексную защиту: как от общих атак, таких как объемный DDoS, так и от атак, которые могут быть замаскированы или смешаны с легитимным трафиком. Все это вместе с возможностью интеграции с WAF позволяет клиентам смягчать последствия атак, выполняемых на сетевом, транспортном и прикладном уровнях стека». ***(How botnet attacks work and how to defend against them // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/how-botnet-attacks-work-and-how-to-defend-against-them/). 19.09.2022).***

***

«Поддерживаемые государством китайские хакеры разработали вариант Linux для бэкдора SideWalk, используемого против систем Windows, принадлежащих целям в академическом секторе.

Вредонос с высокой степенью достоверности приписывается группе угроз SparklingGoblin, также отслеживаемой как Earth Baku, которая, как считается, связана с группой кибершпионажа APT41.

Бэкдор SideWalk Linux наблюдался в прошлом, первоначально его отслеживали как StageClient исследователи безопасности из компании по кибербезопасности ESET.

Ранний вариант вредоносного ПО был обнаружен исследователями из 360 Netlab, группы по анализу угроз китайской компании по обеспечению интернет-безопасности Qihoo 360, и подробно описан два года назад в блоге о ботнете Spectre, поражающем IP-камеры.

Проанализировав Spectre и StageClient, исследователи ESET определили, что оба вредоносных компонента имеют один и тот же корень и являются вариантами SideWalk для Linux.

В 2021 году исследователи Trend Micro задокументировали новые инструменты из кампании кибершпионажа, приписываемые APT41/Earth Baku, включая бэкдор SideWalk, который они отслеживают как ScrambleCross.

ESET отмечает в сегодняшнем отчете, что, хотя SideWalk Linux в прошлом использовался против нескольких целей, их данные телеметрии показывают, что обнаруженный ими вариант был развернут только против одной жертвы в феврале 2021 года, университета в Гонконге.

SparkGoblin сосредоточился на той же цели в прошлом, скомпрометировав тот же университет в мае 2020 года во время студенческих протестов.

Хотя SparklingGoblin в основном атакует цели в Восточной и Юго-Восточной Азии, группа также наносит удары по организациям за пределами этих регионов, сосредоточив внимание на академическом секторе.

SideWalk для Windows готов для Linux

Глядя на варианты SideWalk для Linux и Windows, ESET заметила «поразительное» сходство в том, как они функционируют, в реализации нескольких компонентов и полезных нагрузках, сброшенных на скомпрометированную систему.

Исследователи говорят, что в обоих вариантах реализован алгоритм шифрования ChaCha20 для «использования счетчика с начальным значением 0x0B», что характерно для SideWalk.

Как в Windows, так и в Linux вредоносное ПО использует одни и те же пять потоков, выполняемых одновременно, для определенных задач:

[StageClient::ThreadNetworkReverse] — получение конфигураций прокси для альтернативных подключений к серверу управления и контроля (C2)

[StageClient::ThreadHeartDetect] - закрыть соединение с сервером C2, если команды не получены в указанное время

[StageClient::ThreadPollingDriven] — отправлять контрольные команды на сервер C2, если нет информации для доставки

[StageClient::ThreadBizMsgSend] — проверить наличие данных для отправки в очередях сообщений для всех остальных потоков и обработать их

[StageClient::ThreadBizMsgHandler] — проверка ожидающих сообщений от сервера C2.

Исследователи ESET также обнаружили, что варианты SideWalk для Linux и Windows имеют одинаковую полезную нагрузку, доставляемую через строку распознавателя тайников, размещенную в файле Google Docs.

Еще одним доказательством связи двух вариантов SideWalk с одним и тем же злоумышленником было то, что они оба использовали один и тот же ключ шифрования для передачи данных с зараженной машины на сервер C2.

SparklingGoblin имеет возможность разрабатывать вредоносное ПО, адаптированное к его потребностям, о чем свидетельствует вариант SideWalk Linux. Тем не менее, группа также имеет доступ к имплантатам, наблюдаемым в операциях, приписываемых другим китайским хакерским группам.

Исследователи ESET говорят, что SparklingGoblin имеет доступ к бэкдору ShadowPad и вредоносному ПО Winnti». ***(Ionut Ilascu. Chinese hackers create Linux version of the SideWalk Windows malware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/chinese-hackers-create-linux-version-of-the-sidewalk-windows-malware/). 14.09.2022).***

***

«Группа китайских хакеров «Webworm» экспериментирует с использованием старых вредоносных программ для новых атак, чтобы избежать установления авторства и снизить операционные расходы.

Веб-червь — это кластер кибершпионажа, активный как минимум с 2017 года и ранее связанный с атаками на ИТ-компании, аэрокосмическую отрасль и поставщиков электроэнергии в России, Грузии и Монголии.

Согласно отчету Symantec, входящего в состав Broadcom Software, злоумышленники в настоящее время тестируют различные модифицированные трояны удаленного доступа (RAT) против поставщиков ИТ-услуг в Азии, чтобы определить их эффективность.

RAT, используемые Webworm сегодня, давно забыты, а их источник циркулирует уже много лет. Тем не менее, инструменты безопасности по-прежнему не обнаруживают их легко, а их уклончивость, обфускация и приемы антианализа остаются актуальными.

Кроме того, использование более старых RAT, которые широко распространены и развернуты различными случайными хакерами, помогает веб-червям маскировать свои операции и смешиваться с действиями других, что значительно усложняет работу аналитиков безопасности.

Первое старое вредоносное ПО, используемое в новых операциях веб-червей, — это Trochilus RAT, впервые появившееся в дикой природе в 2015 году и теперь бесплатно доступное через GitHub.

Модификация, добавленная в Trochilus, заключается в том, что теперь он может загружать свою конфигурацию из файла, проверяя набор жестко заданных каталогов.

Второй испытанный штамм — 9002 RAT, популярный вредоносный код среди спонсируемых государством субъектов в предыдущем десятилетии, которые ценили его за способность внедряться в память и работать скрытно.

Веб-червь добавил более надежное шифрование в протокол связи 9002 RAT, чтобы помочь избежать обнаружения современными инструментами анализа трафика.

Третье семейство, используемое в наблюдаемых атаках, — это Gh0st RAT, впервые обнаруженное в 2008 году, которое несколько APT неоднократно использовали в прошлых глобальных операциях кибершпионажа.

Gh0st RAT имеет несколько уровней обфускации, обход UAC, распаковку шелл-кода и запуск в памяти, многие из которых сохранены в версии Webworm.

В отчете Positive Technologies от мая 2022 года модифицированное вредоносное ПО было названо «Deed RAT», приписывая его китайской группе под названием «Космические пираты», которая, по словам Symantec, скорее всего, является той же группой, что и Webworm.

Одной из новых функций Deed RAT, которая по сути является модифицированной версией Gh0st RAT, является универсальная система связи C2, поддерживающая несколько протоколов, включая TCP, TLS, HTTP, HTTPS, UDP и DNS.

Даже если Space Pirates и Webworm являются отдельными группами, известно, что китайские субъекты делятся вредоносными программами, чтобы скрыть их следы и сократить расходы на разработку». ***(Bill Toulas. Webworm hackers modify old malware in new attacks to evade attribution // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/webworm-hackers-modify-old-malware-in-new-attacks-to-evade-attribution/). 15.09.2022).***

***

«Новый пакет вредоносных программ использует каналы жертв на YouTube для загрузки вредоносных видеоуроков, рекламирующих поддельные читы и взломщики для популярных видеоигр, с целью дальнейшего распространения вредоносного пакета.

Самораспространяющийся пакет вредоносного ПО рекламировался в видеороликах на YouTube, предназначенных для фанатов, играющих в FIFA, Final Fantasy, Forza Horizon, Lego Star Wars и Spider-Man.

Эти загруженные видео содержат ссылки для загрузки поддельных кряков и читов, но на самом деле они устанавливают тот же самый самораспространяющийся пакет вредоносных программ, который заразил загрузчика.

В новом отчете «Лаборатории Касперского» исследователи обнаружили RAR-архив, содержащий набор вредоносных программ, в первую очередь RedLine, который в настоящее время является одним из самых массово распространенных похитителей информации.

RedLine может украсть информацию, хранящуюся в веб-браузере жертвы, такую как файлы cookie, пароли к учетным записям и кредитным картам, получить доступ к разговорам в мессенджерах и взломать криптовалютные кошельки.

Кроме того, в RAR-архив включен майнер, использующий видеокарту жертвы, которая, скорее всего, есть у жертвы, поскольку они смотрят игровые видеоролики на YouTube, для добычи криптовалюты для злоумышленников.

Благодаря включенной в комплект легитимной утилите Nirsoft NirCmd под названием «nir.exe» при запуске все исполняемые файлы будут скрыты и не будут генерировать окна в интерфейсе или какие-либо значки на панели задач, поэтому все остается скрытым от жертвы.

Связанные инфекции и исполняемые файлы сами по себе не представляют особого интереса и обычно используются злоумышленниками в других кампаниях по распространению вредоносных программ.

Самораспространяющаяся RedLine через YouTube

Однако «Лаборатория Касперского» обнаружила спрятанный в архиве необычный и интересный механизм самораспространения, который позволяет вредоносной программе самораспространяться на других жертв в Интернете.

В частности, RAR содержит пакетные файлы, которые запускают три вредоносных исполняемых файла, а именно «MakiseKurisu.exe», «download.exe» и «upload.exe», которые выполняют самораспространение пакета.

Первый, MakiseKurisu, представляет собой модифицированную версию широко доступного похитителя паролей C#, используемого исключительно для извлечения файлов cookie из браузеров и их локального хранения.

Второй исполняемый файл, «download.exe», используется для загрузки видео с YouTube, которое является копией видеороликов, рекламирующих вредоносный пакет.

Видео загружаются по ссылкам, полученным из репозитория GitHub, чтобы не указывать URL-адреса видео, о которых сообщалось и которые были удалены с YouTube.

Наконец, «upload.exe» используется для загрузки видеороликов, продвигающих вредоносное ПО, на YouTube, с использованием украденных файлов cookie для входа в учетную запись YouTube жертвы и распространения пакета через их канал.

«Он [upload.exe] использует библиотеку Puppeteer Node, которая предоставляет высокоуровневый API для управления Chrome и Microsoft Edge с использованием протокола DevTools», — поясняет Касперский в отчете.

«Когда видео успешно загружено на YouTube, upload.exe отправляет сообщение в Discord со ссылкой на загруженное видео».

В то время как злоумышленник получает информацию о новой загрузке, владелец канала вряд ли поймет, что он продвигает вредоносное ПО на YouTube, если он не очень активен на платформе.

Этот агрессивный метод распространения еще больше усложняет проверку и удаление на YouTube, поскольку видео, указывающие на вредоносные загрузки, загружаются из учетных записей, которые, вероятно, уже давно имеют незарегистрированную репутацию». ***(Bill Toulas. New malware bundle self-spreads through YouTube gaming videos // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-malware-bundle-self-spreads-through-youtube-gaming-videos/). 15.09.2022).***

***

«VMware и Microsoft предупреждают о продолжающейся широко распространенной вредоносной кампании Chromeloader, которая превратилась в более опасную угрозу, в некоторых случаях наблюдается удаление вредоносных расширений браузера, вредоносных программ node-WebKit и даже программ-вымогателей.

В первом квартале 2022 года резко выросло количество заражений Chromeloader, и исследователи из Red Canary предупредили об опасности угонщика браузера, используемого для маркетинговой аффилиации и мошенничества с рекламой.

Тогда вредоносное ПО заразило Chrome вредоносным расширением, которое перенаправляло пользовательский трафик на рекламные сайты для мошенничества с кликами и получения дохода для злоумышленников.

Несколько месяцев спустя подразделение 42 Palo Alto Network заметило, что Chromeloader превратился в похититель информации, пытаясь выкрасть данные, хранящиеся в браузерах, сохраняя при этом свои рекламные функции.

В пятницу вечером Microsoft предупредила о «продолжающейся широкомасштабной кампании по мошенничеству с кликами», приписываемой злоумышленнику, отслеживаемому как DEV-0796, который использует Chromeloader для заражения жертв различными вредоносными программами.

Сегодня аналитики VMware опубликовали технический отчет с описанием различных вариантов Chromeloader, которые использовались в августе и в этом месяце, некоторые из которых содержат гораздо более мощные полезные нагрузки.

Вредоносная программа ChromeLoader поставляется в виде файлов ISO, которые распространяются через вредоносную рекламу, перенаправления браузера и комментарии к видео на YouTube.

Файлы ISO стали популярным способом распространения вредоносных программ с тех пор, как Microsoft по умолчанию начала блокировать макросы Office. Кроме того, при двойном щелчке по ISO-образу в Windows 10 и более поздних версиях они автоматически монтируются как компакт-диски с новой буквой диска, что делает их эффективным способом одновременного распространения нескольких вредоносных файлов.

ISO-образы ChromeLoader обычно содержат четыре файла: ZIP-архив, содержащий вредоносное ПО, файл ICON, пакетный файл (обычно называемый Resources.bat), который устанавливает вредоносное ПО, и ярлык Windows, запускающий пакетный файл.

В рамках своего исследования VMware протестировала не менее десяти вариантов Chromeloader с начала года, наиболее интересные из которых появились после августа.

Первый пример — программа, имитирующая OpenSubtitles, утилиту, помогающую пользователям находить субтитры для фильмов и телепередач. В этой кампании злоумышленники отказались от своего обычного файла «Resources.bat» и переключились на файл с именем «properties.bat», используемый для установки вредоносного ПО и обеспечения устойчивости путем добавления ключей реестра.

Другим примечательным случаем является «Flbmusic.exe», имитирующий музыкальный проигрыватель FLB, включающий среду выполнения Electron и позволяющий вредоносному ПО загружать дополнительные модули для сетевого взаимодействия и отслеживания портов.

Для некоторых вариантов атаки оказались немного разрушительными, извлекая ZipBombs, которые перегружают систему массивной операцией распаковки.

«Еще в конце августа было замечено, что ZipBomb сбрасываются на зараженные системы. ZipBomb сбрасывается при первоначальном заражении в архиве, который загружает пользователь. Пользователь должен дважды щелкнуть, чтобы ZipBomb запустилась. После запуска вредоносная программа уничтожает систему пользователя, перегружая ее данными», — поясняется в отчете VMware.

Еще более тревожным является то, что в последних версиях Chromeloader было замечено развертывание программы-вымогателя Enigma в HTML-файле.

Enigma — это старая разновидность программы-вымогателя, использующая установщик на основе JavaScript и встроенный исполняемый файл, поэтому его можно запускать непосредственно из браузера по умолчанию.

После завершения шифрования к файлам добавляется расширение «.enigma», а программа-вымогатель оставляет файл « readme.txt », содержащий инструкции для жертв.

Поскольку рекламное ПО не наносит заметного ущерба системам жертв, кроме того, что оно потребляет часть полосы пропускания, аналитики обычно игнорируют или преуменьшают его значение.

Тем не менее, каждое программное обеспечение, которое внедряется в системы без обнаружения, является кандидатом на более серьезные проблемы, поскольку его авторы могут применять модификации, которые облегчают более агрессивные варианты монетизации.

Хотя Chromeloader начинался как рекламное ПО, он является прекрасным примером того, как злоумышленники экспериментируют с более мощными полезными нагрузками, изучая более прибыльные альтернативы мошенничеству с рекламой». ***(Bill Toulas. VMware, Microsoft warn of widespread Chromeloader malware attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/vmware-microsoft-warn-of-widespread-chromeloader-malware-attacks/). 19.09.2022).***

***

«Угроза Metador нацелена на телекоммуникационные компании, интернет-провайдеров и университеты

Невиданный ранее продвинутый злоумышленник по имени Метадор нацелен на телекоммуникации, интернет-провайдеров и университеты в нескольких странах Ближнего Востока и Африки для кибершпионажа.

Исследователи SentinelLabs обнаружили, что операторы, стоящие за Metador, были осведомлены о «безопасности операций, управлении тщательно сегментированной инфраструктурой для каждой жертвы и быстром развертывании

сложных контрмер при наличии решений безопасности» и обеспечивают долгосрочный доступ к сетям несколькими избыточными способами.

«Мы назвали этого злоумышленника «Metador» в связи со строкой «I am meta» в одном из образцов вредоносного ПО и ожиданием ответов на испанском языке от командно-контрольных серверов», — говорят исследователи.

Критические выводы

Исследователи обнаружили две разные вредоносные платформы на базе Windows, называемые metaMain и Mafalda, которые в основном используются Metador для работы полностью в памяти и избегания обнаружения собственной системы безопасности.

По словам исследователей SentinelLabs, metaMain — это многофункциональный бэкдор. Операторы Метадора использовали его имплантат для расшифровки в памяти последующей модульной структуры под названием Мафальда. Mafalda также является многофункциональным бэкдором.

Исследователи говорят, что имплантат metaMain обеспечивает долгосрочный доступ к скомпрометированным машинам и предоставляет операторам такие функции, как регистрация событий клавиатуры и мыши, кража скриншотов, загрузка и выгрузка файлов, а также возможность запуска произвольного шелл-кода.

Mafalda — это интерактивный имплантат, поддерживающий более 60 команд и очень ценный актив для операторов Метадора, а новые варианты демонстрируют интенсивную запутанность, что затрудняет их анализ.

«Внутренние версии Mafalda предполагают, что эта платформа использовалась в течение некоторого времени, а ее адаптируемость только во время нашего взаимодействия подчеркивает активную и непрерывную разработку», — говорят исследователи.

Они также обнаружили признаки дополнительных имплантатов, в том числе:

Cryshell, специальный имплантат, используемый для передачи соединений во внутренней сети на внешние серверы управления и контроля;

Неизвестное вредоносное ПО для Linux, используемое для кражи материалов с других компьютеров в целевой среде и перенаправления их коллекции обратно в Mafalda.

Исследователи говорят, что атрибуция Metador была «искаженной загадкой» и что они столкнулись с несколькими языками с различными особенностями, указывающими на нескольких разработчиков.

«Следы указывают на множество разработчиков и операторов, говорящих как на английском, так и на испанском языках, наряду с различными культурными отсылками, включая лирику британского поп-панка и аргентинские политические карикатуры», — говорят исследователи SentinelLabs Хуан Андрес Герреро-Сааде, Амитай Бен Шушан Эрлих и Александр Миленкоски.

Они также обнаружили, что имплантат Mafalda обеспечивает функции, аналогичные metaMain, и является активно поддерживаемым текущим проектом. Исследователи наблюдали два ключевых варианта бэкдора Mafalda — «Clear Build 144» и «Запутанный вариант Mafalda».

Вариант Obfuscated Mafalda расширяет поддерживаемые команды с 54 до 67 и изобилует методами антианализа.

Исследователи также обнаружили, что Mafalda печатает зашифрованные сообщения отладчика, если имя хоста — WIN-K4C3EKBSMMI, что, возможно, указывает на имя компьютера, используемого разработчиками.

По словам исследователей, этот бэкдор Mafalda является текущим проектом. Всего было просмотрено 67 команд, и 13 из них были добавлены в более новом варианте.

Некоторые из интересных команд в новом варианте Mafalda включают в себя:

Команда 55, которая копирует файл или каталог из исходной файловой системы, предоставленной злоумышленником, в указанную атакующим папку целевой файловой системы;

Команда 60, которая считывает содержимое %USERPROFILE%AppDataLocalGoogleChromeUser DataLocal State и отправляет его в команду и управление с именем с префиксом «loot»;

Команда 63, которая проводит разведку конфигурации сети и системы;

Команда 67, которая помогает получить данные от другого имплантата, находящегося в сети жертвы, и отправить данные на C2.

Команды Mafalda включают кражу учетных данных, кражу данных и информации, выполнение команд, манипулирование системным реестром и файловой системой, а также реконфигурацию Mafalda.

Исследователи также заметили, что операторы, стоящие за вторжениями Metador, используют один внешний IP-адрес для каждой сети жертвы, который используется для управления и контроля либо через HTTP, либо через необработанный TCP. Они обнаружили, что серверы были размещены на LITESERVER, голландском хостинг-провайдере». ***(Prajeet Nair. Metador Threat Group Targets Telcos, ISPs and Universities // Information Security Media Group, Corp. (https://www.govinfosecurity.com/metador-threat-group-targets-telcos-isps-universities-a-20141). 24.09.2022).***

***

«Хакеры, предположительно работающие на Россию, начали использовать новую технику выполнения кода, основанную на движении мыши в презентациях Microsoft PowerPoint, для запуска вредоносного скрипта PowerShell.

Вредоносный макрос не требуется для выполнения вредоносного кода и загрузки полезной нагрузки для более коварной атаки.

В отчете компании по анализу угроз Cluster25 говорится, что APT28 (также известная как «Fancy Bear»), группа угроз, приписываемая российскому ГРУ (Главное разведывательное управление Генерального штаба России), использовала новую технику для доставки вредоносного ПО Graphite совсем недавно. 9 сентября.

Злоумышленник заманивает цели с помощью файла PowerPoint (.PPT), предположительно связанного с Организацией экономического сотрудничества и развития (ОЭСР), межправительственной организацией, работающей над стимулированием экономического прогресса и торговли во всем мире.

Внутри файла PPT есть два слайда с инструкциями на английском и французском языках по использованию параметра «Интерпретация» в приложении для видеоконференций Zoom.

Файл PPT содержит гиперссылку, которая действует как триггер для запуска вредоносного сценария PowerShell с помощью утилиты SyncAppvPublishingServer. Этот метод документирован с июня 2017 года. В то время несколько исследователей объясняли, как заражение работает без вредоносного макроса, вложенного в документ Office.

Основываясь на найденных метаданных, Cluster25 сообщает, что хакеры готовили кампанию в период с января по февраль, хотя URL-адреса, использованные в атаках, были активны в августе и сентябре.

Исследователи говорят, что субъект угрозы нацелен на организации в оборонном и государственном секторах стран Европейского Союза и Восточной Европы, и считают, что шпионская кампания продолжается.

Цепочка заражения

Когда жертва открывает документ-приманку в режиме презентации и наводит указатель мыши на гиперссылку, активируется вредоносный сценарий PowerShell для загрузки файла JPEG («DSC0002.jpeg») из учетной записи Microsoft OneDrive.

JPEG представляет собой зашифрованный DLL-файл (lmapi2.dll), который расшифровывается и помещается в каталог «C:\ProgramData\», а затем выполняется через rundll32.exe. Раздел реестра для сохраняемости также создается для библиотеки DLL.

Затем lmapi2.dll извлекает и расшифровывает второй файл JPEG и загружает его в память в новом потоке, ранее созданном библиотекой DLL.

Cluster25 уточняет, что для каждой строки во вновь извлеченном файле требуется отдельный ключ XOR для деобфускации. В результате полезная нагрузка представляет собой вредоносное ПО Graphite в форме переносимого исполняемого файла (PE).

Graphite злоупотребляет API Microsoft Graph и OneDrive для связи с сервером управления и контроля (C2). Злоумышленник получает доступ к службе, используя фиксированный идентификатор клиента, чтобы получить действительный токен OAuth2.

Исследователи объясняют, что с новым токеном OAuth2 Graphite запрашивает у Microsoft GraphAPI новые команды, перечисляя дочерние файлы в подкаталоге check OneDrive.

«Если обнаруживается новый файл, контент загружается и расшифровывается с помощью алгоритма дешифрования AES-256-CBC», — говорит Cluster25, добавляя, что «вредоносная программа позволяет удаленно выполнять команды, выделяя новую область памяти и выполняя полученный шелл-код с помощью вызов нового выделенного потока».

Цель вредоносного ПО Graphite — позволить злоумышленнику загрузить другие вредоносные программы в системную память. Это было задокументировано еще в январе исследователями из Trellix, слияния McAfee Enterprise и FireEye, которые назвали его так специально, потому что он использует API Microsoft Graph для использования OneDrive в качестве C2.

Кампания, которую расследовала Trellix, использовала документы Excel под названиями «parliament_rew.xlsx» и «Misions Budget.xlsx», которые, по-видимому, были нацелены на государственных служащих и отдельных лиц в оборонной промышленности.

Основываясь на сходстве кода с образцами вредоносного ПО за 2018 год, таргетинге и инфраструктуре, используемой в атаках, Trellix приписал Graphite APT28 с низкой или средней степенью достоверности». ***(Bill Toulas. Hackers use PowerPoint files for 'mouseover' malware delivery // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-use-powerpoint-files-for-mouseover-malware-delivery/). 26.09.2022).***

***

«Новое вредоносное ПО для кражи информации Erbium распространяется как поддельные взломщики и читы для популярных видеоигр с целью кражи учетных данных жертв и криптовалютных кошельков.

Erbium — это новое вредоносное ПО как услуга (MaaS), которое предоставляет подписчикам новую вредоносную программу для кражи информации, которая набирает популярность в сообществе киберпреступников благодаря своей обширной функциональности, поддержке клиентов и конкурентоспособным ценам.

Исследователи из команды Cluster25 были первыми, кто сообщил об Erbium ранее в этом месяце, но в новом отчете Cyfirma содержится дополнительная информация о том, как распространяется троян для кражи паролей.

Новая операция «Вредоносное ПО как услуга»

Erbium продвигается на русскоязычных форумах с июля 2022 года, но его фактическое использование в дикой природе до сих пор остается неопределенным.

Первоначально эрбий стоил 9 долларов в неделю, но, поскольку его популярность выросла в конце августа, цена выросла до 100 долларов в месяц или 1000 долларов за годовую лицензию.

По сравнению с «де-факто» выбором в этой области, похитителем RedLine, стоимость Erbium составляет примерно одну треть, поэтому он направлен на то, чтобы разрушить рынок вредоносных программ, обычно используемых злоумышленниками.

Как и другие вредоносные программы для кражи информации, Erbium похищает данные, хранящиеся в веб-браузерах (на основе Chromium или Gecko), такие как пароли, файлы cookie, кредитные карты и информацию автозаполнения.

Вредоносная программа также пытается извлечь данные из большого набора криптовалютных кошельков, установленных в веб-браузерах в качестве расширений.

Также украдены холодные настольные кошельки, такие как Exodus, Atomic, Armory, Bitecoin-Core, Bytecoin, Dash-Core, Electrum, Electron, Coinomi, Ethereum, Litecoin-Core, Monero-Core, Zcash и Jaxx.

Erbium также крадет коды двухфакторной аутентификации из Trezor Password Manager, EOS Authenticator, Authy 2FA и Authenticator 2FA.

Вредоносное ПО может захватывать скриншоты со всех мониторов, похищать токены Steam и Discord, красть файлы аутентификации Telegram и профилировать хост на основе ОС и оборудования.

Все данные передаются на C2 через встроенную систему API, а операторы получают обзор того, что было украдено с каждого зараженного хоста, на панели инструментов Erbium…

Вредоносное ПО использует три URL-адреса для подключения к панели, включая сеть доставки контента (CDN) Discord, платформу, которой операторы вредоносного ПО активно злоупотребляют.

Хотя Erbium все еще находится в стадии разработки, пользователи хакерских форумов высоко оценили усилия автора и его готовность прислушиваться к запросам клиентов.

Cluster25 сообщил о признаках заражения эрбием по всему миру, в том числе в США, Франции, Колумбии, Испании, Италии, Индии, Вьетнаме и Малайзии.

В то время как первая кампания Erbium использует игровые кряки в качестве приманки, каналы распространения могут значительно диверсифицироваться в любое время, поскольку покупатели вредоносного ПО могут использовать разные методы для его продвижения.

Чтобы не допустить угрозы в вашу систему, избегайте загрузки пиратского программного обеспечения, сканируйте все загруженные файлы с помощью антивирусного инструмента и обновляйте свое программное обеспечение, устанавливая последние доступные исправления безопасности». ***(Bill Toulas. New Erbium password-stealing malware spreads as game cracks, cheats // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-erbium-password-stealing-malware-spreads-as-game-cracks-cheats/). 26.09.2022).***

***

Програми-вимагачі

«Группа LockBit, занимающаяся программами-вымогателями как услугой, выплатила первый платеж в размере 50 000 долларов США в рамках своей программы вознаграждения за обнаружение ошибок для исследователей, желающих помочь в борьбе с киберпреступностью.

Коллектив вымогателей объявил в июне, что будет платить людям, которые найдут уязвимости, которые можно использовать, а также ошибки в программном обеспечении, которое оно использует для злонамеренного шифрования файлов, что позволит жертвам спасти свои данные.

Согласно Darkfeed, платформе поставщика услуг по мониторингу программ-вымогателей, 6 июля была предложена первая награда за сообщение об ошибке в программном обеспечении для шифрования, которое было исправлено в тот же день.

По словам группы, ошибка позволяла бесплатно расшифровывать форматы виртуальных дисков, такие как файлы VMDK или VHDX, поскольку эти файлы начинаются с нулей.

По данным Darkfeed, говорится в сообщении группы, «для минимизации ущерба и влияния платежей за дешифратор от текущих атакованных компаний было принято решение отложить публичное объявление награды до текущего дня».

Когда LockBit объявила о своей программе вознаграждения за обнаружение ошибок в июне, она заявила: «Мы приглашаем всех исследователей безопасности, этичных и неэтичных хакеров на планете принять участие в нашей программе вознаграждения за обнаружение ошибок. Сумма вознаграждения варьируется от 1000 до 1 миллиона долларов»...

Плодовитая банда вымогателей связала объявление о своей награде с выпуском новой версии улучшенного вредоносного ПО LockBit 3.0.

Bug bounty — это программы, предназначенные для поощрения ответственного раскрытия уязвимостей путем побуждения исследователей отправлять свои выводы ответственному поставщику.

Группа вымогателей поблагодарила неизвестного лауреата и смогла внести изменения в свой алгоритм шифрования в шифраторе файлов Linux VMDK и снова зашифровать все файлы.

Он также поблагодарил агента ФБР и сотрудника Coveware за предоставление инсайдерской информации, которая позволила злоумышленникам-вымогателям узнать о «слабых местах и ошибках в системах шифрования наших конкурентов».

С февраля по март число известных жертв программ-вымогателей выросло со 185 до 283, сообщила в марте консалтинговая компания NCC Group...

Судя по выявленным атакам, LockBit 2.0 был самым результативным, на него пришлось 96 из 283 атак, за ним следуют Conti с 71 атакой, Hive с 26 атаками и BlackCat, также известный как Alphv, с 23 атаками, сообщает NCC Group. Из известных жертв 44% проживают в Северной Америке, за ними следуют Европа с 38% и Азия с 7%, добавляет он». ***(Prajeet Nair. Ransomware-as-a-Service Gang LockBit Pays First $50K Bounty // Information Security Media Group, Corp. (https://www.govinfosecurity.com/ransomware-as-a-service-gang-lockbit-pays-first-50k-bounty-a-20099). 18.09.2022).***

***

«Ряд атак программ-вымогателей в Чили и Черногории нанес значительный ущерб, закрыв банки и правительственные учреждения и даже побудив партнеров Организации Североатлантического договора (НАТО) обратиться за экстренной помощью.

Черногория сталкивается с продолжающейся жестокой кампанией атак программ-вымогателей, которые, как представляется, исходят от преступных группировок в России и нацелены на правительственные веб-сайты. Черногория, член НАТО с 2017 года, обратилась к США за помощью в отражении этих атак. Правительственные учреждения в Чили также пострадали от новой формы программ-вымогателей, нацеленных на серверы Linux, и по крайней мере одному из них угрожали «двойным вымогательством» свалки украденной информации.

Правительственные учреждения пострадали от очень разрушительных атак программ-вымогателей, обнаружен один совершенно новый штамм

Черногория получает поддержку от группы кибербезопасности ФБР после того, как ряд правительственных веб-сайтов подверглись атакам программ-вымогателей и были отключены. Нападения кажутся оппортунистическими, поскольку они происходят в период политических волнений в стране, когда действующее правительство было свергнуто в середине августа в результате вотума недоверия. Тем не менее, еще не установлено участие поддерживаемых государством передовых групп постоянной угрозы; кажется, что атаки программ-вымогателей исходят из России, но на данный момент они кажутся делом рук преступных групп, стремящихся получить прибыль.

Тем не менее связи с Россией побудили агентство национальной безопасности страны обратиться за защитой к НАТО. Европейский союз также заявил о своей поддержке, организовав «многострановой проект», который направит в страну экспертов для оказания помощи в защите ее критически важной инфраструктуры.

Злоумышленники используют программу-вымогатель Cuba, которая была привязана к центральной группе, работающей по схеме «программа-вымогатель как услуга». Он был в обращении с начала 2020 года, но атака в Черногории содержит новый компонент: новый вирус под названием «Zero Date», который исследователи безопасности все еще изучают.

Атака в Черногории привела к отключению нескольких правительственных учреждений, как сообщается, из-за предосторожности, поскольку проблема устраняется. Министерства обороны, финансов и внутренних дел (среди прочих) не работали несколько дней. Атаки программ-вымогателей в некоторых случаях сочетались с распределенными атаками типа «отказ в обслуживании» (DDoS) — метод, который вызывает больше подозрений в отношении операции российского правительства, но также не является чем-то неслыханным в криминальных кругах. Сообщается, что электросеть страны на некоторое время была переведена на ручное управление в результате одной из таких DDoS-атак.

Посольство США в столице страны предупреждает путешественников, что кампания может нарушить работу международных перевозок, коммунальных услуг и телекоммуникаций на неопределенный период времени. Правительство Черногории заявило, что личные данные граждан не были скомпрометированы, но некоторые услуги (например, сбор налогов с розничной торговли) могут быть на некоторое время нарушены. Злоумышленники утверждают, что взломали здание парламента страны и похитили исходный код, финансовые документы, переписку с банковскими служащими и налоговые документы среди прочего.

Чили отразила аналогичные атаки программ-вымогателей

Правительственные учреждения Чили также сильно пострадали от атак программ-вымогателей, но, по всей видимости, от другого злоумышленника, использующего совершенно новую разновидность программы-вымогателя, нацеленную на серверы под управлением Linux.

В стране говорится, что по крайней мере одно неназванное государственное учреждение было отключено в конце августа, а злоумышленник потребовал выплатить выкуп в течение трех дней под угрозой продажи данных другим преступникам через темную сеть. Группа реагирования на инциденты компьютерной безопасности страны (CSIRT) заявила, что новый штамм, название которого еще не

названо, обладает способностью обходить автоматизированную защиту и шифровать съемные устройства в дополнение к обнаружению известных недостатков в серверах Microsoft и VMware ESXi.

Хотя сохраняется вероятность того, что за одной или обеими этими атаками стоит поддерживаемая государством группа APT, в последнее время банды вымогателей проявляют повышенную готовность атаковать правительственные учреждения. В частности, кажется, что они нацелены на небольшие правительства, у которых может не быть ИТ-ресурсов, чтобы справиться с шквалом атак. Недавнее нападение банды Конти на правительство Коста-Рики является прекрасным примером того, насколько наглыми стали эти группы; эта атака на несколько недель нанесла ущерб различным государственным службам, но, как сообщается, Конти совершила ее скорее как рекламный ход, чем серьезная попытка получить выкуп.

Существует также проблема чувства патриотизма со стороны преступных группировок, базирующихся в России; некоторые открыто заявили, что будут помогать своему правительству после начала вторжения в Украину. Даже если они не получают прямых указаний из Москвы, некоторые из этих атак могут быть мотивированы войной.

Другие недавние нападения на правительственные учреждения произошли в Аргентине, Доминиканской Республике и Бразилии. В комментарии Сэма Карри, директора службы безопасности Cybereason, отмечается, что громкие атаки такого рода имели место и в ряде других стран: «В Греции на прошлой неделе крупнейший в стране поставщик природного газа подвергся атаке со стороны банды вымогателей Ragnar Locker».

«На Тайване всплыла массовая DDoS-атака, потому что это быстрый и удобный инструмент для быстрых результатов и обычных ингредиентов, которые могут сопровождать более серьезные и вложенные атаки. Кибертеррористы и банды вымогателей наносят удары по этим странам и операторам критической инфраструктуры, потому что считают их уязвимыми. Учитывая безрассудные нападения на Черногорию, все страны должны быть в состоянии повышенной готовности, независимо от того, насколько они географически или политически близки к украинско-российскому конфликту», — сказал Карри. «Чтобы защититься от DDoS-атак и программ-вымогателей, организации как государственного, так и частного секторов должны подготовиться в мирное время и обеспечить избыточность сетевого подключения, а также иметь готовые стратегии смягчения последствий. И не только готовьтесь к объемным атакам (существует больше видов DDoS, чем к простым наводнениям), но также соблюдайте гигиену безопасности и регулярно обновляйте и исправляйте операционные системы и другое программное обеспечение. Кроме того, проводите периодические командно-штабные учения и учения с привлечением людей, не входящих в группу безопасности, вплоть до Представительского люкса». ***(Scott Ikeda. Devastating Ransomware Attacks on Chile, Montenegro Shut Down Government Agencies, Banks // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/devastating-ransomware-attacks-on-chile-montenegro-shut-down-government-agencies-banks/). 06.09.2022).***

***

«2021 год был годом программ-вымогателей, количество атак увеличилось почти вдвое по сравнению с 2020 годом.

Он уже имел тенденцию к росту до пандемии, но когда деловой мир внезапно массово перешел на удаленную работу, киберпреступники ухватились за возможность использовать недавно обнаруженные уязвимости, возникающие в гибридной рабочей среде.

Сотрудники, работающие на дому, стали основными мишенями для злоумышленников, и количество успешных взломов программ-вымогателей резко возросло. Как и стоимость восстановления данных.

Последние отчеты показывают, что средняя общая стоимость утечки данных увеличилась более чем на 10% в 2021 году, с 3,86 млн долларов до 4,24 млн долларов, что является самым высоким показателем за всю историю наблюдений.

В подавляющем большинстве случаев страховка покрывала эти расходы для бизнеса, включая выплату выкупа. Однако 2022 год — это совсем другая история. Так же, как ландшафт угроз кибербезопасности быстро изменился за последний год, рынок киберстрахования тоже изменился.

Поставщики страховых услуг в области кибербезопасности, оправившись от исторической пары лет, совершенствуют свои квалификационные процессы и поднимают планку выплат, поэтому предприятия больше не могут полагаться только на страхование в качестве стратегии защиты и восстановления.

Потребность в сложном учебнике по кибербезопасности, в котором люди, процессы и технологии работают вместе для достижения цели «предотвращения», как никогда актуальна. Также необходимо настроить процессы на случай сбоя технологии или нахождения киберпреступником обходного пути, включая упреждающий мониторинг, быстрое обнаружение, немедленное реагирование и сдерживание. Страхование остается только в качестве экстренного «лекарства», поскольку киберустойчивость никогда не была так важна для бизнеса.

Новый вымогатель «Дикий Запад»

Захватывающие заголовки и очень прибыльные успехи, достигнутые глобальными кибер-бандами с помощью программ-вымогателей, не остались незамеченными. И это привело к притоку на рынок новых, часто менее опытных игроков, ищущих собственные возможности.

Проблема в том, что не все банды киберпреступников одинаковы.

Предыдущие разработчики программ-вымогателей действовали с таким уровнем сложности и технических возможностей, которые позволяли им не только украсть и сохранить данные фирмы, но и выпустить их без изменений после выплаты выкупа.

Они действуют как предприятия, предлагая программу-вымогатель как услугу (RaaS) и продавая свой код в даркнете тому, кто больше заплатит. Побочный эффект заключается в том, что это снизило входной барьер для новой волны преступных группировок.

И мало того, что этим новым игрокам-мошенникам не хватает навыков и знаний того же уровня для управления такого рода сложным предприятием, они также менее заинтересованы в том, чтобы играть по правилам, установленным известными бандами, такими как GandCrab. Существует реальная опасность того,

что жертвы класса '22 и выше могут заплатить выкуп, а их данные не будут возвращены. Если они заплатят выкуп хотя бы один раз, компании также рискуют снова стать мишенью, так как это демонстрация слабости по отношению к киберпреступникам.

Данные бесценны, и их потеря может нанести ущерб бизнесу. И даже самая дорогая страховка не может его вернуть.

Таким образом, единственный жизнеспособный способ предотвратить это — предотвратить нарушение в первую очередь. Это означает внедрение передовых методов кибербезопасности.

Рост страховой волны поднимает все стандарты

По большей части компании, ставшие жертвами программ-вымогателей, платят выкуп. Это только подтолкнуло злоумышленников к более активным атакам, а косвенный эффект заставил страховых компаний пересмотреть свои предложения по страховым полисам.

Страховые компании реагируют на растущее число требований либо повышением цен на свои полисы, либо отказом покрывать определенные направления атак, чтобы не остаться в кармане. Например, лондонская компания Lloyd's исключила атаки на государства из своей страховки, а AXA France, крупная европейская страховая компания, вообще прекратила покрытие платежей программ-вымогателей. Многие страховые компании по всему миру вдвое сократили сумму страхового покрытия, которое они предоставляют после пандемии, а удаленная работа вызвала всплеск атак программ-вымогателей, которые заставили их вздрогнуть от огромных выплат.

Это повышение цен и порогов выплат страховой отраслью оказывает положительное скрытое влияние на деловой мир. Это вынуждает фирмы переоценивать свои средства защиты, слабые стороны и обеспечивать наличие передовых методов защиты от кибербезопасности. Это также повышает осведомленность о кибербезопасности в организациях.

Поскольку основная роль страховщиков заключается в измерении рисков, им требуются доказательства того, что компании готовы противостоять будущим атакам, что побуждает предприятия повышать свои стандарты.

Этот один-два удара более строгих страховых полисов и рост цен, наряду с появлением новых игроков-вымогателей «Дикий Запад», являются тревожным сигналом, который нужен многим предприятиям, чтобы не рассматривать страхование как одеяло безопасности.

Чтобы не пострадать и остаться на ногах, предприятия должны взять на себя обязательство покончить со своей чрезмерной уверенностью в страховании и сосредоточить упреждающие меры для защиты своих данных.

Одной из ключевых технологий, которую следует учитывать, является расширенное обнаружение и реагирование (XDR).

Большая видимость в мире удаленной работы

XDR повышает прозрачность операций по обеспечению безопасности и повышает эффективность групп защиты. Эти решения предоставляют больше источников данных и дают командам по безопасности больше контекста в их стеке,

улучшая и поддерживая работу существующих синих команд за счет лучшего понимания типов угроз, векторов атак и масштабов атак в организации.

XDR также предоставляет вашим командам по безопасности инструменты, необходимые им для остановки атаки и ее анализа, путем проведения перекрестной корреляции угроз на основе их поведения и индикатора компрометации (IOC) во всей среде, чтобы обеспечить актуальность и готовность вашей защиты, чтобы помешать следующему. XDR также расширяет возможности решений Managed Detection and Response (MDR), которые уже есть у многих компаний, и сочетание этих двух технологий имеет решающее значение для предотвращения атак на ранних стадиях и предотвращения успешных атак программ-вымогателей.

Киберстрахование все больше становится тем, что организациям, вероятно, потребуется иметь. Но, как и страхование автомобиля и жилья, оно покрывает только наихудший сценарий. Наличие страховки автомобиля и жилья не означает, что вы не должны безопасно управлять автомобилем или запирать двери и окна. Точно так же киберстрахование не означает, что компании не должны иметь надежную и упреждающую систему безопасности.

Когда дело доходит до денег, нарушения обходятся компаниям дороже, чем их страховые взносы, поскольку помимо потери данных и процесса восстановления, компании также платят за восстановление, репутационный ущерб и штрафы регулирующих органов. Рост затрат обычно не является положительным моментом, но в этом случае растущие взносы на киберстрахование могут быть просто исключением. Это должно стать призывом к действию для всех компаний, чтобы срочно пересмотреть свои протоколы кибербезопасности и убедиться, что их команды оснащены для выявления, сообщения и устранения угроз, чтобы переход от реактивного восстановления к проактивному предотвращению и киберустойчивости». ***(Danny O'Neill. Prevention Is Better Than Cure: Ransomware Insurance Is Not a Cybersecurity Strategy // Rezonen Pte. Ltd. (https://www.cpomagazine.com/cyber-security/prevention-is-better-than-cure-ransomware-insurance-is-not-a-cybersecurity-strategy/). 13.09.2022).***

***

«В августе в GRIT наблюдалась небольшая тенденция к снижению общего количества сообщений о программах-вымогателях (со 187 до 176, падение на 5,88%), при этом в восьми группах было зарегистрировано снижение количества сообщений по сравнению с июлем. В частности, у шести групп количество публичных сообщений сократилось на 50% и более, включая Yanlouwang, Hive, Lorenz, AlphV, Onyx и Cuba. Группа вымогателей Hive была особенно примечательна из-за того, что их жертвы сократились с 26 жертв в июле до всего 7 жертв в августе.

Всего 6 августа поступило 22 сообщения, что на два больше, чем самый высокий наблюдаемый день в июле, и это наибольшее количество сообщений, наблюдаемых за один день с конца апреля.

Несмотря на небольшое снижение общего числа публично размещенных жертв, в августе количество активных групп увеличилось на 19%. Donut Leaks и IceFire впервые сообщили о жертвах, и мы также видели некоторые утечки от групп,

которые не проявляли активности в июле, включая Snatch, Daixin и RansomEXX. И наоборот, 0mega и Red Alert были единственными группами, активными в июле, которые не заявили о жертвах в августе.

Технологии и производство оказались наиболее затронутыми отраслевыми вертикалями, каждая из которых поднялась на одну позицию и обогнала розничную и оптовую торговлю. Фактически, в отраслях продуктов питания и напитков, недвижимости, розничной и оптовой торговли, а также в СМИ и рекламе наблюдалось самое большое снижение таргетинга по сравнению с июлем, в то время как в фармацевтике, образовании и здравоохранении наблюдался резкий рост по сравнению с июлем.

Вертикаль «Производство» уже восемь месяцев находится в тройке лидеров, и это второй месяц подряд, когда Технологии находятся в первой тройке, и четвертый месяц — в первой тройке.

Среди основных целевых отраслей наиболее активными группами были LockBit, IceFire и BianLian, а основными целевыми странами были США, Германия, Швейцария и Великобритания. Примечательно, что технологии и производство остаются двумя наиболее пострадавшими вертикалями даже после исключения США из пула данных.

По состоянию на конец августа в нескольких странах, включая Турцию (в первую очередь из-за жертв IceFire), в Соединенном Королевстве, Германии и США наблюдалось наибольшее увеличение общего таргетинга во всех отраслях, в то время как такие страны, как Франция, Австралия, Нидерланды и Объединенные Арабские Эмираты, небольшой перерыв с уменьшением числа жертв программ-вымогателей.

В целом, в августе GRIT наблюдал таргетинг против 35 из 40 отслеживаемых стран. На Соединенные Штаты приходилось 71,4% атак на гусеничные отрасли, что намного больше, чем в любой другой стране (следующей по количеству целевых стран является Великобритания с 17,1%). Наиболее активно нацеленными на США группами были LockBit, Blackbasta и Bianlian.

Lockbit по-прежнему остается самой плодовитой группой программ-вымогателей на сегодняшний день, и их число заявленных жертв в месяц продолжает расти по мере продвижения к 2022 году. У Lockbit число заявленных жертв увеличилось на 8,3% с июля по август с 65 отчетами. Доминирование Lockbit подчеркивает Блэкбаста, которая заняла второе место, несмотря на то, что опубликовала только один день, в общей сложности 17 жертв (на 22,7% меньше, чем в июле). Бяньлянь, новый претендент по состоянию на июль, занял 3-е место с 12 жертвами за последние три дня месяца.

Впервые IceFire был замечен исследователями MalwareHunterTeam в марте 2022 года, и в то время они не использовали сайт утечки. В августе IceFire начал операции по двойному вымогательству с использованием сайта утечки, и уже в первый день работы на сайте было зарегистрировано более 40 жертв. Примерно в то же время начали появляться сообщения на форуме BleepingComputer с просьбой помочь с программой-вымогателем IceFire.

Публично раскрытые жертвы IceFire в значительной степени сосредоточены на технологической отрасли и представляют необычные целевые страны, включая Турцию, Иран, Пакистан и Объединенные Арабские Эмираты.

Примечательно, что недавно они добавили функцию «Сделать доказательство», при которой жертвы могут заплатить ровно 1 XMR, чтобы расшифровать один файл в качестве доказательства того, что группа может расшифровать зашифрованные файлы. Это чрезвычайно необычная тактика, так как самые изощренные группы вымогателей обычно предоставляют доказательства, расшифровывая небольшие файлы бесплатно.

Заявленные ими жертвы совпадают с профилями жертв других организаций-вымогателей, что предполагает возможную связь между аффилированными лицами в нескольких группах, пытающихся получить дополнительный доход, угрожая опубликовать данные отдельно от своей аффилированной группы вымогателей.

Последние мысли

В целом август, по-видимому, немного замедлился в широкомасштабной активности среди устоявшихся групп вымогателей. Lockbit остается самой плодовитой группой программ-вымогателей и сохраняет сильное лидерство среди злоумышленников: в августе ежемесячно сообщалось о жертвах на 8% больше. С другой стороны, в Hive, AlphV и Blackbasta наблюдалось значительное снижение общего числа зарегистрированных жертв: с июля по август они упали на 73%, 57% и 23% соответственно.

Среди целевых стран 17 стран, которые были выбраны в июле, не попали в таргетинг в августе, включая страны Европы, Африки, Ближнего Востока и Восточной Азии. В качестве альтернативы, 16 стран, не затронутых в июле, стали мишенями в августе. Эти сдвиги предполагают, что многие жертвы становятся мишенью для аффилиатов различных групп вымогателей.

Несмотря на замедление в августе, в 2022 году программы-вымогатели, вероятно, продолжат оставаться одной из самых серьезных угроз, с которыми сталкиваются организации. По мере того, как мы приближаемся к сентябрю и к концу третьего квартала, GRIT продолжит отслеживать новые тенденции в области электронных преступлений и программ-вымогателей. ***(Drew Schmitt. GRIT Ransomware Report: August 2022 // Techstrong Group Inc. (https://securityboulevard.com/2022/09/grit-ransomware-report-august-2022/). 15.09.2022).***

***

Программы-вымогатели — одна из самых серьезных проблем кибербезопасности, с которыми мы сталкиваемся сегодня, поскольку киберпреступники взламывают предприятия, школы, больницы, критически важную инфраструктуру и многое другое, чтобы зашифровать файлы и потребовать выкуп за ключ дешифрования.

Несмотря на предупреждения, многие жертвы платят эти выкупы, полагая, что это самый быстрый способ восстановить их сеть, особенно если киберпреступники также угрожают утечкой украденных данных. Но все это означает, что цикл атак продолжается, и группы вымогателей используют свои нечестно полученные доходы для финансирования более амбициозных атак.

Помимо этого есть еще одна проблема. Многие инциденты с программами-вымогателями просто держатся в секрете, поэтому сложно получить четкое

представление о том, что на самом деле происходит в мире. Даже когда компании признаются в кибератаке, они очень часто не имеют четкого представления о том, что произошло, и, похоже, крайне неохотно называют какой-либо инцидент атакой программы-вымогателя.

«Серьезная кибератака», «кибер-инцидент, вызвавший некоторые сбои» и «данные, зашифрованные третьей стороной» — это лишь некоторые из заявлений, сделанных жертвами атак программ-вымогателей для описания того, что произошло, — но никогда упоминание программ-вымогателей.

Некоторые жертвы в конечном итоге становятся более открытыми в отношении того, что произошло, но только спустя месяцы или годы после инцидента, а некоторые вообще публично не признают, что это была программа-вымогатель.

Разочаровывает невозможность получить исчерпывающую и четкую картину происходящего — даже если, читая между строк расплывчатые заявления о «сложном киберинциденте», который «нарушил работу служб», становится ясно, что это атака программы-вымогателя.

А отсутствие прозрачности в отношении атак программ-вымогателей и других киберинцидентов наносит ущерб всем.

Некоторые жертвы очень быстро сообщают, что это программа-вымогатель, и я брал интервью у жертв атак программ-вымогателей, которые после того, как инцидент миновал, готовы говорить под запись о том, что произошло, и интересно услышать, как ИТ-директора и директора по информационной безопасности рассказывают о том, что произошло.

Общая черта среди этих лидеров кибербезопасности, которые решили рассказать об организациях, пострадавших от программ-вымогателей, заключается в том, что они хотят помочь не допустить, чтобы другие стали следующей жертвой, подробно изложив уроки, которые они извлекли из укрепления киберзащиты для предотвращения будущих инцидентов.

Такие уроки, как своевременное применение исправлений безопасности, предоставление пользователям по сети многофакторной аутентификации (MFA), а также регулярное обновление резервных копий, — это шаги, которые могут помочь остановить атаки программ-вымогателей. И лучшее время для принятия мер — до того, как произойдет нападение.

«Программы-вымогатели — это не только техническая проблема: в конечном счете, эти кибератаки затрагивают всех, и мы часто остаемся в неведении относительно того, почему службы, на которые мы полагаемся, не работают.

В некоторых случаях кажется, что это уже меняется. Недавно Los Angeles Unified (LAUSD), второй по величине школьный округ в США, подвергся атаке программы-вымогателя, что немедленно сообщило об инциденте властям, а также информировало широкую общественность о ситуации.

Их подход был высоко оценен директором Агентства кибербезопасности и безопасности инфраструктуры (CISA) Джен Истерли, которая сказала, что LAUSD «четко осознает ценность прозрачности при реагировании на киберинцидент - их скорость, ясность и нацеленность на партнерство достойны похвалы», и описала их.

как «отличный пример того, как информировать заинтересованные стороны, в том числе о потенциальных последствиях и о том, чего ожидать дальше».

Борьба с атакой программ-вымогателей — непростая задача, но то, как организации формируют опыт, так же важно, как и технический ответ. Подробно описывая, что произошло и как разрешился инцидент, они могут получить положительную обратную связь и показать, что групп вымогателей не всегда следует опасаться.

И это просто может помешать другим постичь ту же участь. В борьбе с программами-вымогателями будет лучше для всех, если атаки будут более прозрачными». ***(Danny Palmer. The ransomware problem won't get better until we change one thing // ZDNET (https://www.zdnet.com/article/the-ransomware-problem-wont-get-better-until-we-change-one-thing/). 11.09.2022).***

***

«Если вы пострадали от программы-вымогателя LockerGoga, международные правоохранительные органы опубликовали инструмент для решения этой проблемы.

LockerGoga — это вредоносное программное обеспечение для Windows, стоящее за заражением Norsk Hydro в 2019 году, которое отключило глобальную сеть норвежского энергетического и металлургического гиганта на неделю и обошлось компании более чем в 100 миллионов долларов, не говоря уже о побочных эффектах в цепочке поставок.

Файлы с расширением «.locked» являются индикатором того, что LockerGoga зашифровала ваши документы, и могут быть восстановлены без оплаты, согласно Bitdefender, который работал с Европолом, правоохранительными органами Цюриха и проектом NoMoreRansom над уже доступным инструментом дешифрования..

Служба безопасности также опубликовала пошаговое руководство [PDF] о том, как использовать дешифратор на отдельных компьютерах и компьютерах, подключенных к сети.

В дополнение к продвижению инструмента дешифратора, правоохранительные органы Цюриха опубликовали подробности об уголовном преследовании против злоумышленника, которого они обвинили в том, что он был частью банды киберпреступников, которая использовала программы-вымогатели LockerGoga и MegaCortext для заражения компьютеров, используемых более чем 1800 людьми и организациями в 71 стране. причинение предполагаемого ущерба на общую сумму в сотни миллионов долларов.

Предполагаемый преступник был арестован швейцарскими властями в октябре 2021 года по подозрению в отмывании денег и искажении данных. Его арест был частью более крупной операции Европола и Агентства Европейского Союза по сотрудничеству в области уголовного правосудия (Евроюст), в ходе которой были задержаны 12 подозреваемых киберпреступников и в которых участвовали правоохранительные органы Франции, Нидерландов, Норвегии, Украины, США и Швейцарии.

С тех пор кибергруппа полиции Цюриха оценивает улики, изъятые во время обыска дома подозреваемого, и это расследование выявило «многочисленные закрытые ключи от атак программ-вымогателей», как нам сказали.

Эти ключи помогли некоторым компаниям-жертвам восстановить свои данные, ранее зашифрованные программой-вымогателем LockerGoga или MegaCortex, а также привели к выпуску дешифратора LockerGoga.

По данным правоохранительных органов Цюриха, аналогичный инструмент, помогающий жертвам MegaCortex расшифровывать свои файлы, будет выпущен «в ближайшее время».

MegaCortex, который также впервые появился в 2019 году, включает в себя подписанный исполняемый файл Windows как часть полезной нагрузки и предназначен для корпораций, согласно более раннему исследованию, опубликованному TrendMicro.

Между тем, этот прибыльный вид киберпреступности не проявляет никаких признаков замедления, поскольку в последние недели банды вымогателей опустились до новых минимумов, нанося удары по школам и больницам, среди других жертв.

Согласно отчету Verizon о расследовании нарушений данных за 2022 год, опубликованному в мае, на программы- вымогатели приходилось 25 процентов наблюдаемых инцидентов безопасности, произошедших в период с 1 ноября 2020 года по 31 октября 2021 года, и они присутствовали в 70 процентах всех заражений вредоносным ПО.

Авторы отчета отмечают, что количество вспышек программ-вымогателей увеличилось на 13 процентов по сравнению с прошлым годом, что больше, чем за предыдущие пять лет вместе взятые». ***(Jessica Lyons Hardcastle. Been hit by LockerGoga ransomware? A free fix is now out // The Register (https://www.theregister.com/2022/09/19/lockergoga_ransomware_decryptor/).19.09.2022).***

***

«Все большее число групп вымогателей используют новую тактику, которая помогает им быстрее шифровать системы своих жертв, снижая при этом шансы быть обнаруженными и остановленными.

Эта тактика называется прерывистым шифрованием и состоит в шифровании только части содержимого целевых файлов, что по-прежнему делает данные невосстановимыми без использования действительного дешифратора + ключа.

Например, пропуская каждые следующие 16 байт файла, процесс шифрования занимает почти половину времени, необходимого для полного шифрования, но при этом блокирует содержимое навсегда.

Кроме того, поскольку шифрование является более мягким, автоматические инструменты обнаружения, которые полагаются на обнаружение признаков проблем в виде интенсивных операций ввода-вывода файлов, с большей вероятностью потерпят неудачу.

SentinelLabs опубликовал отчет, в котором изучается тенденция, начатая LockFile в середине 2021 года и в настоящее время принятая такими компаниями, как Black Basta, ALPHV (BlackCat), PLAY, Agenda и Qyick.

Эти группы активно продвигают наличие периодических функций шифрования в своем семействе программ-вымогателей, чтобы побудить аффилированных лиц присоединиться к операции RaaS.

«Примечательно, что Qyick использует прерывистое шифрование, которое используют крутые ребята, пока вы читаете это. В сочетании с тем фактом, что он написан на Go, скорость не имеет себе равных», — говорится в рекламе Qyick на хакерских форумах.

Программа-вымогатель Agenda предлагает прерывистое шифрование в качестве дополнительного и настраиваемого параметра. Три возможных режима частичного шифрования:

skip-step [skip: N, step: Y] — Шифровать каждые Y МБ файла, пропуская N МБ.

fast [f:N] - Зашифровать первые N МБ файла.

процент [n: N; p:P] — шифровать каждые N МБ файла, пропуская P МБ, где P равно P% от общего размера файла.

Реализация прерывистого шифрования в BlackCat также предоставляет операторам возможность выбора конфигурации в виде различных шаблонов пропуска байтов.

Например, вредоносное ПО может шифровать только первые байты файла, следовать точечному шаблону, проценту блоков файла, а также имеет «автоматический» режим, объединяющий несколько режимов для получения более запутанного результата.

Недавнее появление программы-вымогателя PLAY в результате громкой атаки на аргентинскую судебную систему Кордовы также было подкреплено скоростью прерывистого шифрования.

PLAY не дает параметров конфигурации, а вместо этого просто разбивает файл на 2, 3 или 5 фрагментов, в зависимости от размера файла, а затем шифрует каждый другой фрагмент.

Наконец, Black Basta, одно из самых громких имен в этой области на данный момент, также не дает операторам возможности выбирать между режимами, поскольку его напряжение решает, что делать, в зависимости от размера файла.

Для небольших файлов размером менее 704 байт он шифрует все содержимое. Для файлов размером от 704 байт до 4 КБ он шифрует 64 байта и пропускает 192 байта между ними.

Если размер файла превышает 4 КБ, программа-вымогатель Black Basta уменьшает размер нетронутых интервалов до 128 байт, в то время как размер зашифрованной части остается равным 64 байтам.

Прерывистое шифрование, по-видимому, имеет значительные преимущества и практически не имеет недостатков, поэтому аналитики безопасности ожидают, что в ближайшее время этот подход перейдет к большему числу групп вымогателей.

Штамм LockBit уже является самым быстрым с точки зрения скорости шифрования, поэтому, если банда примет технику частичного шифрования, продолжительность ее ударов сократится до пары минут.

Конечно, шифрование — сложный вопрос, и прерывистое шифрование должно выполняться правильно, чтобы гарантировать, что оно не приведет к легкому восстановлению данных жертвами.

На данный момент реализация BlackCat является наиболее сложной, а реализация Qyick остается неизвестной, поскольку аналитики вредоносных программ еще не проанализировали образцы нового RaaS». ***(Bill Toulas. Ransomware gangs switching to new intermittent encryption tactic // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ransomware-gangs-switching-to-new-intermittent-encryption-tactic/). 10.09.2022).***

***

«Банда вымогателей Lorenz теперь использует критическую уязвимость в устройствах Mitel MiVoice VOIP для взлома предприятий, используя их телефонные системы для первоначального доступа к своим корпоративным сетям.

Исследователи безопасности Arctic Wolf Labs заметили эту новую тактику после того, как заметили значительное совпадение с тактиками, методами и процедурами (TTP), связанными с атаками программ-вымогателей, использующих ошибку CVE-2022-29499 для первоначального доступа, как сообщал Crowdstrike в июне.

Хотя эти инциденты не были связаны с конкретной бандой вымогателей, Arctic Wolf Labs смогла с высокой степенью уверенности приписать аналогичную вредоносную деятельность банде Lorenz.

«Первоначальная вредоносная активность исходила от устройства Mitel, расположенного на сетевом периметре», — сообщили исследователи безопасности в опубликованном сегодня отчете.

«Лоренц использовал CVE-2022-29499, уязвимость удаленного выполнения кода, влияющую на компонент Mitel Service Appliance MiVoice Connect, чтобы получить обратную оболочку, а затем использовал Chisel в качестве инструмента туннелирования для перехода в среду».

Это важное дополнение к арсеналу банды, учитывая, что продукты Mitel Voice-over-IP (VoIP) используются организациями в критически важных секторах по всему миру (включая правительственные учреждения), и в настоящее время более 19 000 устройств подвергаются атакам через Интернет. эксперт Кевин Бомонт.

Mitel устранил уязвимость, выпустив исправления безопасности в начале июня 2022 года после выпуска сценария исправления для уязвимых версий MiVoice Connect в апреле.

Злоумышленники недавно использовали другие недостатки безопасности, влияющие на устройства Mitel, в рекордных DDoS - атаках с усилением.

Группа вымогателей Lorenz нацелена на корпоративные организации по всему миру как минимум с декабря 2020 года, требуя выкуп в сотни тысяч долларов от каждой жертвы.

Майкл Гиллеспи из ID Ransomware сообщил BleepingComputer, что шифратор Lorenz такой же, как тот, который использовался предыдущей операцией по вымогательству, известной как ThunderCrypt.

Эта банда также известна тем, что продает данные, украденные до шифрования, другим злоумышленникам, чтобы заставить своих жертв заплатить выкуп и продавать доступ к внутренним сетям своих жертв другим киберпреступникам вместе с украденными данными.

Если выкуп не выплачивается после утечки украденных данных в виде защищенных паролем архивов RAR, Лоренц также выпускает пароль для доступа к украденным архивам, чтобы обеспечить публичный доступ к украденным файлам.

В июне 2021 года голландская фирма по кибербезопасности Tesorion выпустила бесплатный дешифратор программ-вымогателей Lorenz, который можно использовать для восстановления некоторых типов файлов, включая документы Office, файлы PDF, изображения и видео.

Список предыдущих жертв включает Hensoldt, многонационального оборонного подрядчика со штаб-квартирой в Германии, и Canada Post, основного почтового оператора в Канаде». ***(Sergiu Gatlan. Lorenz ransomware breaches corporate network via phone systems // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/lorenz-ransomware-breaches-corporate-network-via-phone-systems/). 12.09.2022).***

***

«Согласно отчету SpyCloud о защите от программ-вымогателей за 2022 год, несмотря на увеличение инвестиций в инструменты для борьбы с программами-вымогателями, 90% организаций в той или иной степени пострадали от программ-вымогателей за последние 12 месяцев.

Респонденты оценили риск атаки через сторонних поставщиков как основной фактор, определяющий распределение бюджетов на безопасность, за которым следует рост частоты и изощренность атак программ-вымогателей. В результате решения организаций по борьбе с программами-вымогателями все больше фокусируются на риске захвата учетной записи как предвестнике этой формы кибератаки.

Количество организаций, которые внедрили или планируют внедрить многофакторную аутентификацию, подскочило на 71% с 56% в предыдущем году до 96%. Мониторинг скомпрометированных учетных данных сотрудников также увеличился с 44% до 73%.

По мере того, как организации укрепляют свою гигиену паролей и вкладывают средства в такие инструменты, как MFA, преступники удваивают и расширяют традиционные тактики, чтобы обойти их защиту. Например, развертывание вредоносных программ на персональных устройствах для доступа к корпоративным приложениям или перехват сеансов с использованием скомпрометированных файлов cookie может позволить преступникам полностью обойти процесс аутентификации.

«Многофакторная аутентификация обеспечивает столь необходимый дополнительный уровень безопасности, но он не идеален. Недавно мы услышали предостережения против использования SMS-аутентификации для MFA, поскольку тексты могут быть перехвачены мотивированными киберпреступниками, но даже push-уведомления и приложения аутентификации не являются полностью

надежными или безопасными, о чем свидетельствуют тенденции этих вредоносных программ и скомпрометированных файлов cookie», — Даррен Сигел, Cyber Security. Об этом в Help Net Security рассказал эксперт Specops Software.

«Этот отчет о защите является отличным напоминанием о необходимости обучения сотрудников вопросам безопасности и улучшения контроля безопасности. Необходимо регулярно проводить обучение по кибербезопасности для всех сотрудников, чтобы научить их распознавать угрозы кибербезопасности и то, как они могут помочь смягчить их — такие вещи, как дважды подумать, прежде чем щелкнуть ссылку или одобрить уведомление MFA и установить более надежные пароли».

Меры кибербезопасности не могут закрыть пробелы

Эта недавняя тактика преступников в конечном итоге не привела к снижению общего числа киберинцидентов. На самом деле, опрос показал, что организации не только все еще становятся жертвами, но и имеют все большую вероятность быть атакованными более одного раза: 50% подверглись атакам как минимум дважды, 20,3% подверглись атакам от 6 до 10 раз и 7,4% подверглись атакам более 10 раз.

«Организации правильно обеспокоены невольными внутренними угрозами — их меры кибербезопасности не в состоянии устранить бреши, ведущие к атакам программ-вымогателей», — сказал генеральный директор SpyCloud Тед Росс. «Организации могут не знать, что незамеченное заражение вредоносным ПО на персональных устройствах представляет собой наиболее опасную из этих брешей. Этот отчет показывает, что организации тратят время и деньги на решения, которые оставляют конфиденциальные данные открытыми. Даже если службы безопасности получат данные своих организаций, как только они будут распространены в темной сети, преступники могут использовать их для более разрушительных действий, включая их следующую атаку».

Заражение вредоносным ПО

Заражение вредоносным ПО распространено шире, чем думают многие организации. Проанализировав журналы ботнетов, повторно захваченные только в этом году, исследователи SpyCloud выявили более 6 миллионов зараженных вредоносным ПО устройств с перехваченными учетными данными приложений.

Киберпреступники развертывают вредоносное ПО для кражи данных, включая учетные данные для приложений рабочей силы, отпечатки пальцев браузера и файлы cookie устройства или веб-сеанса, что позволяет им выдавать себя за сотрудника, получать доступ и шифровать данные, обходя MFA и другие меры безопасности.

В среднем в 2022 году исследователи SpyCloud обнаружили от 16 до 26 уникальных уязвимых приложений или доменов на зараженное устройство, что составляет от 96 до 156 миллионов перехваченных учетных данных для входа в приложения. Хотя очистка зараженного устройства может помешать преступникам получить доступ к большему количеству данных, она не устраняет раскрытие более широкой личности и не предотвращает доступ к предприятию в будущем. Надежное восстановление после заражения имеет решающее значение, поскольку повторное создание образа зараженного устройства без исправления приложений оставляет большой пробел в системе безопасности предприятия.

По мнению 87 % респондентов, сообщения о вредоносных программах для кражи учетных данных, таких как RedLine Stealer, повысили обеспокоенность их организаций неконтролируемыми личными устройствами как потенциальной точкой входа для программ-вымогателей. Неуправляемые устройства вызывают серьезную озабоченность, поскольку службы безопасности не могут отслеживать их на наличие таких угроз, как вредоносное ПО и воздействие сторонних приложений. В результате киберзащитники не видят всей поверхности своих атак и поэтому часто недооценивают свои риски, связанные с вредоносным ПО.

Стратегии предотвращения программ-вымогателей

«Эффективные стратегии предотвращения программ-вымогателей должны быть сосредоточены на точках входа, которые специалисты по безопасности не могут видеть, — скрытой поверхности атаки, которая включает в себя сторонние приложения и неуправляемые машины, находящиеся за пределами их стандартной компетенции мониторинга», — сказал Росс. «Одно устройство, зараженное вредоносным ПО, может поставить под угрозу сотни корпоративных приложений. Даже после того, как вредоносное ПО будет удалено, ущерб будет нанесен, если все эти приложения не будут должным образом исправлены после заражения — в противном случае двери остаются открытыми для программ-вымогателей и других критических угроз для предприятия».

В связанных новостях несколько штатов США недавно приняли решение запретить местным и государственным агентствам и организациям, финансируемым за счет долларов налогоплательщиков, платить бандам вымогателей, и еще несколько штатов готовятся к этому. Чтобы узнать больше об этом, у нас есть видео, в котором рассказывается о возможных последствиях такого законодательства и, в целом, о развивающемся характере атак программ-вымогателей и текущих глобальных усилиях, направленных на борьбу с угрозами программ-вымогателей». ***(The various ways ransomware impacts your organization // Help Net Security (https://www.helpnetsecurity.com/2022/09/27/various-ways-ransomware-impacts-your-organization/). 27.09.2022).***

***

«Относительно новая банда вымогателей Bl00Dy начала использовать недавно просочившийся сборщик программ-вымогателей LockBit для атак на компании.

На прошлой неделе в Твиттер просочилась программа-вымогатель LockBit 3.0 после того, как оператор LockBit поссорился со своим разработчиком. Этот конструктор позволяет любому создать полнофункциональный шифратор и дешифратор, который злоумышленники могут использовать для атак.

Поскольку сборщик включает в себя файл конфигурации, который можно легко настроить для использования различных заметок о выкупе, серверов статистики и функций, BleepingComputer предсказал, что другие злоумышленники вскоре будут использовать сборщик для создания своих собственных программ-вымогателей.

К сожалению, наши прогнозы сбылись, и относительно новая группа программ-вымогателей под названием «Bl00Dy Ransomware Gang» уже использовала конструктор для атаки на украинскую организацию.

Банда вымогателей Bl00dy

Как впервые сообщил DataBreaches.net, банда вымогателей Bl00Dy начала действовать примерно в мае 2022 года, когда они атаковали группу медицинских и стоматологических кабинетов в Нью-Йорке.

Как и в случае с другими программами-вымогателями, управляемыми людьми, злоумышленники взламывают сеть, крадут корпоративные данные и шифруют устройства. Однако вместо того, чтобы использовать сайт утечки данных Tor для вымогательства жертв и публикации украденных данных, злоумышленники используют для той же цели канал Telegram.

Хотя это явно банда «вымогателей», злоумышленники, похоже, не разрабатывают программы-вымогатели независимо друг от друга. Вместо этого они создают шифровальщики, используя утекшие сборщики и исходный код других операций вымогателей, таких как Babuk [VirusTotal] и Conti [VirusTotal].

В понедельник исследователь кибербезопасности Владислав Радецкий опубликовал отчет о новом шифровальщике Bl00Dy Ransomware Gang, который был обнаружен при атаке на украинскую жертву.

Однако было неясно, была ли программа-вымогатель основана на Conti или LockBit, поскольку электронное письмо «filedecryptionsupport@msgsafe.io» ранее было в шифраторе, созданном на основе просочившегося исходного кода Conti.

Позже исследователь MalwareHunterTeam подтвердил, что шифровальщик был построен с использованием недавно выпущенного компоновщика LockBit 3.0. Сканирование Intezer также показало много совпадений кода между шифровальщиками Bl00dy и LockBit 3.0.

BleepingComputer протестировал шифровальщик Bl00dy Ransomware Gang и обнаружил некоторые различия между этим новым шифровальщиком и предыдущими.

В прошлых кампаниях злоумышленники добавляли расширение.bl00dy для зашифрованных файлов. Однако, поскольку это не настраиваемый параметр в сборщике LockBit 3.0, злоумышленникам остается использовать расширения, определенные при сборке шифровальщика.

Что касается примечания о выкупе, имена файлов по-прежнему создаются в стиле LockBit, но злоумышленники настроили их так, чтобы они включали собственный текст и контактную информацию…

В конечном счете, это шифровальщик программ-вымогателей LockBit 3.0, поэтому он поддерживает все функции, о которых ранее сообщали исследователи безопасности.

Неудивительно, что Bl00dy Ransomware Gang переключается между семействами программ-вымогателей по мере необходимости, чтобы либо избежать обнаружения, либо воспользоваться различными функциями.

Операция LockBit была запущена в сентябре 2019 года и с тех пор превратилась в одну из самых активных и многофункциональных операций Ransomware-as-a-Service на данный момент.

LockBit 3.0 был выпущен в июне 2022 года с новой тактикой вымогательства, переработанным шифровальщиком с использованием кода от BlackMatter и первой программой вознаграждения за ошибки программ-вымогателей.

Поскольку просочившийся конструктор программ-вымогателей LockBit 3.0 легко настраивается другими злоумышленниками, вскоре мы увидим, как другие злоумышленники будут использовать его в своих собственных атаках». ***(Lawrence Abrams. Leaked LockBit 3.0 builder used by 'Bl00dy' ransomware gang in attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/leaked-lockbit-30-builder-used-by-bl00dy-ransomware-gang-in-attacks/). 28.09.2022).***

***

Програми-трояни

«Северокорейские хакеры используют троянские версии SSH-клиента PuTTY для развертывания бэкдоров на целевых устройствах в рамках фальшивой оценки работы Amazon.

Новым элементом этой кампании является использование троянской версии утилиты PuTTY и KiTTY SSH для развертывания бэкдора, которым в данном случае является «AIRDRY.V2».

Согласно техническому отчету Mandiant, опубликованному сегодня, кластером угроз, ответственным за эту кампанию, является «UNC4034» (он же «Temp.Hermit» или «Labyrinth Chollima»).

Последние действия группы, похоже, являются продолжением кампании Operation Dream Job, которая проводится с июня 2020 года и на этот раз нацелена на медиакомпании.

«В июле 2022 года в ходе упреждающего поиска угроз в компании, работающей в медиа-индустрии, Mandiant Managed Defense выявила новую методологию целевого фишинга, используемую кластером угроз, отслеживаемым как UNC4034», — пояснил Mandiant.

Атака начинается с того, что злоумышленники обращаются к своим целям по электронной почте с выгодным предложением о работе в Amazon, а затем отправляют сообщение в WhatsApp, где они делятся файлом ISO («amazon_assessment.iso»).

ISO включает текстовый файл («readme.txt»), содержащий IP-адрес и учетные данные для входа, а также троянскую версию PuTTY (PuTTY.exe), очень популярного консольного приложения SSH с открытым исходным кодом.

BleepingComputer также знает о злоумышленниках, которые выдают себя за клиента KiTTY SSH, ответвление PuTTY, используя имя файла «Amazon-KiTTY.exe».

Хотя неясно, какие обсуждения происходили между злоумышленниками и жертвами, хакеры, вероятно, сказали жертве открыть ISO-образ и использовать прилагаемый инструмент SSH и учетные данные для подключения к хосту и выполнить оценку навыков.

Однако PuTTY, которым поделились хакеры, был изменен, чтобы включить вредоносную полезную нагрузку в свой раздел данных, что сделало измененную версию значительно больше, чем законную версию.

Поскольку исполняемый файл PuTTY был скомпилирован из легитимной программы, он полностью функционален и выглядит точно так же, как легитимная версия.

Однако хакеры модифицировали connect_to_host() функцию PuTTY таким образом, что при успешном подключении SSH с использованием прилагаемых учетных данных программа развертывает вредоносную полезную нагрузку шелл-кода DAVESHELL в виде библиотеки DLL ("colorui.dll"), упакованной с Themida.

Чтобы сделать запуск шеллкода незаметным, вредоносный PuTTY использует уязвимость перехвата порядка поиска в «colorcpl.exe», законном инструменте управления цветом Windows, для загрузки вредоносной DLL.

DAVESHELL действует как дроппер последней полезной нагрузки, бэкдора AIRDRY.V2, который выполняется непосредственно в памяти.

AIRDRY.V2 может взаимодействовать через HTTP, файл или SMB через именованный канал, пытаясь подключиться к одному из трех жестко запрограммированных адресов C2 пять раз, прежде чем перейти в 60-секундный спящий режим.

Хотя у бэкдора есть технические возможности для использования прокси-сервера и отслеживания активных сеансов RDP, в версии, изученной Mandiant, эти функции отключены по умолчанию.

В AIRDRY.V2 поддерживаются следующие девять команд:

Загрузить основную информацию о системе

Обновите интервал маяка на основе значения, предоставленного сервером C2.

Деактивировать до новой даты и времени начала

Загрузить текущую конфигурацию

Обновите конфигурацию

Keep-alive

Обновите интервал маяка на основе значения в конфигурации.

Обновите ключ AES, используемый для шифрования запросов C2 и данных конфигурации.

Загрузите и запустите плагин в памяти

По сравнению с предыдущей версией AIRDRY новый вариант поддерживает меньше команд, но выполнение плагина в памяти и обновление ключа AES для связи C2 — это новые возможности.

Сокращение числа поддерживаемых команд не влияет на универсальность бэкдора, потому что получение плагинов из C2 открывает новый потенциал для более хирургических атак.

Чтобы проверить наличие троянских версий PuTTY, вы можете просмотреть свойства исполняемого файла и убедиться, что он имеет цифровую подпись «Саймон Тэтэм».

К сожалению, законная программа KiTTY обычно не подписывается разработчиком и вместо этого должна быть загружена в службу сканирования на вирусы, такую как VirusTotal, для проверки обнаружения вредоносных программ».

(Bill Toulas. Hackers trojanize PuTTY SSH client to backdoor media company // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-trojanize-putty-ssh-client-to-backdoor-media-company/). 15.09.2022).

***

Фішингові атаки

«За даними компанії з кібербезпеки Securonix, хакери використовують файли з фото з космічного телескопа «Джеймс Вебб» для поширення шкідливих програм на комп'ютерах Windows. Про це йдеться у дослідженні Securonix.

Дослідники виявили модифіковане фото з першої серії знімків космосу від «Вебба», призначене для зараження комп'ютерів.

За даними Securonix, хакери розсилають фішингові електронні листи, що містять офісний документ Microsoft, в якому є «заражене» зображення глибокого космосу. Воно включає шкідливий код Base64.

Після зараження програмне забезпечення дозволяє хакерам контролювати систему жертви.

Голова комісії з альтернативних видів енергії й атомної енергії Франції Етьєн Кляйн 31 липня опублікував нібито фото з телескопа «Джеймс Вебб», на якому, за його словами, зображено Проксиму Центавра.

Пізніше виявилося, що це фото ковбаски чорізо на чорному тлі». ***(Лев Шевченко. Хакери використовують космічні фото для розповсюдження шкідливих програм на Windows // Інформаційне агентство ЛІГАБізнесІнформ (https://tech.liga.net/ua/other/novosti/hakery-ispolzuyut-kosmicheskie-foto-dlya-rasprostraneniya-vredonosnyh-programm-na-windows). 05.09.2022).***

***

«Любая утечка данных начинается с фишинговой атаки. Чтобы ваша организация не стала следующей жертвой, вам необходимо понимать различные типы фишинговых атак и способы их выявления.

Фишинг — это тип кибератаки, при которой используются мошеннические электронные письма или веб-сайты, чтобы обманным путем заставить жертв поделиться конфиденциальной информацией, такой как учетные данные для входа или финансовая информация.

Согласно опросу, 91% кибератак начинаются с фишинговых писем. Существуют разные фишинговые атаки, и каждая из них использует другой метод для обмана жертв.

В этом блоге мы обсудим распространенные типы фишинговых атак и способы их выявления. Итак, читайте дальше, чтобы узнать больше.

Типы фишинговых атак и советы по их выявлению

1) Обманчивый фишинг: электронная почта для массового рынка

Обманчивый фишинг — наиболее распространенный тип фишинговой атаки. Он использует мошеннические электронные письма или веб-сайты, которые

выглядят так, как будто они получены из законного источника, такого как компания или организация.

Злоумышленник обычно подделывает адрес электронной почты или веб-сайт, чтобы они выглядели реальными. Они также могут использовать логотипы или другую графику из законных источников, чтобы электронное письмо или веб-сайт выглядели более убедительно.

Обманчивые фишинговые атаки часто крадут учетные данные для входа, финансовую информацию или другие конфиденциальные данные. Их также можно использовать для установки вредоносных программ на компьютер или устройство жертвы. Проверьте возможности координации вашей организации, когда происходит инцидент

Например, в 2017 году мошенническая фишинговая атака была нацелена на пользователя Netflix. Злоумышленники отправляли электронные письма, которые выглядели так, как будто они были отправлены от Netflix, с просьбой к получателям обновить свою платежную информацию.

Электронное письмо содержало логотип и брендинг Netflix и направляло пользователей на поддельный веб-сайт, который выглядел как настоящий веб-сайт Netflix.

Если пользователи вводили свои платежные данные на поддельном веб-сайте, злоумышленники могли украсть номера их кредитных карт и другие конфиденциальные данные.

Как определить мошеннические фишинговые атаки?

Обманчивые фишинговые атаки бывает сложно идентифицировать, потому что они выглядят как законные электронные письма или веб-сайты. Тем не менее, есть несколько красных флажков, на которые вы можете обратить внимание:

Если вы не ожидаете письма от отправителя, будьте подозрительны.

Если в письме есть грамматические или орфографические ошибки, это может быть фишинговое письмо.

Если электронное письмо или веб-сайт отличаются от обычного формата, это может быть фишинговая атака.

Это всего лишь несколько красных флажков, на которые стоит обратить внимание. Если вы когда-нибудь не уверены в адресе электронной почты или веб-сайте, не нажимайте на ссылки и не вводите какую-либо информацию.

Вместо этого свяжитесь с компанией или организацией напрямую, чтобы подтвердить адрес электронной почты или веб-сайт.

2) Целевой фишинг: персонализированные электронные письма

Целевой фишинг — это фишинговая атака, в которой используются персонализированные электронные письма для целевых лиц или организаций.

Злоумышленник обычно имеет информацию о своих целях, такую как их имя, должность или компания. Они будут использовать эту информацию, чтобы электронное письмо выглядело более убедительно.

Например, в 2016 году целевая фишинговая атака была нацелена на сотрудников Национального комитета Демократической партии (DNC). Злоумышленники отправляли электронные письма, которые выглядели так, как

будто они были отправлены от Google, с просьбой к получателям обновить данные своей учетной записи Google.

Электронное письмо содержало логотип и брендинг Google, направляя пользователей на поддельный веб-сайт, который выглядел как настоящий веб-сайт Google. Если пользователи введут свои учетные данные на поддельном веб-сайте, злоумышленники украдут информацию об их учетной записи.

Как определить целевые фишинговые атаки?

Целевые фишинговые атаки бывает сложно идентифицировать, потому что они часто выглядят как законные электронные письма. Тем не менее, есть несколько красных флажков, на которые вы можете обратить внимание:

Если вы не ожидаете письма от отправителя, будьте подозрительны.

Если в письме есть грамматические или орфографические ошибки, это может быть фишинговое письмо.

Если электронное письмо адресовано вам по имени, это может быть целевой фишинговой атакой.

Все это — красные флажки, которые должны вызвать у вас подозрения в отношении электронной почты. Если вы когда-либо не уверены в электронном письме, не нажимайте на ссылки и не вводите никакой информации. Вместо этого свяжитесь с компанией или организацией напрямую, чтобы подтвердить адрес электронной почты.

3) Китобойный промысел: электронные письма, нацеленные на высокопоставленных лиц

Whaling — это фишинговая атака, в которой электронные письма используются для нацеливания на высокопоставленных лиц, таких как генеральные директора, финансовые директора и другие руководители.

Злоумышленники обычно имеют информацию о своих целях, такую как их имя или должность в компании. Они будут использовать эту информацию, чтобы электронное письмо выглядело более убедительно.

Например, в 2020 году китобойное нападение было совершено против сотрудников крупной американской компании. Злоумышленники отправляли электронные письма, выглядевшие так, как будто они были отправлены генеральным директором компании, с просьбой к получателям перевести деньги на новый банковский счет.

Электронное письмо содержало имя генерального директора и торговую марку, направляя пользователей на поддельный веб-сайт, который выглядел как настоящий веб-сайт компании. Если пользователи введут свои учетные данные на поддельном веб-сайте, злоумышленники украдут информацию об их учетной записи.

Как распознать китобойное нападение?

Китобойные атаки может быть сложно идентифицировать, потому что они часто выглядят как законные электронные письма. Тем не менее, есть несколько красных флажков, на которые вы можете обратить внимание:

К любому электронному письму, в котором вас просят перевести деньги или произвести оплату, следует относиться с подозрением.

Если электронное письмо адресовано вам по имени, это может быть китобойная атака.

Если электронное письмо отправлено высокопоставленным лицом, например генеральным директором или финансовым директором, это может быть китобойная атака.

Злоумышленники часто пытаются подтолкнуть вас к действию, поэтому с подозрением относитесь к любым электронным письмам, в которых вас просят действовать немедленно.

Это общие признаки китобойного нападения. Если вы когда-либо не уверены в электронном письме, не нажимайте на ссылки и не вводите никакой информации. А еще лучше, даже не открывайте письмо. Вместо этого свяжитесь с компанией или организацией напрямую, чтобы подтвердить адрес электронной почты.

4) Фарминг: перенаправление трафика на поддельные сайты

Фарминг — это фишинговая атака, которая использует поддельные веб-сайты, чтобы обманом заставить пользователей ввести свои личные данные.

Злоумышленники обычно рассылают спам-письма, содержащие ссылки на поддельные веб-сайты. Пользователи, которые нажимают на эти ссылки, будут перенаправлены на фальшивый веб-сайт, даже не подозревая об этом.

Поддельный веб-сайт будет выглядеть идентично реальному веб-сайту и иметь тот же бренд и логотип. Однако URL-адрес будет немного другим. Например, фишинговый веб-сайт для Facebook может иметь следующий URL-адрес:

www.faceb00k.com.

Когда пользователи вводят свои учетные данные для входа на поддельный веб-сайт, злоумышленники украдут информацию об их учетной записи.

Как выявить фарм-атаки?

Фарминговые атаки бывает сложно идентифицировать, потому что поддельные веб-сайты выглядят идентично реальным. Тем не менее, есть несколько красных флажков, на которые вы можете обратить внимание:

Прежде чем вводить какую-либо информацию, проверьте URL-адрес веб-сайта. Если URL-адрес отличается от фактического веб-сайта, это может быть фишинговый веб-сайт.

Это может быть фарминговая атака, если вас перенаправляют на веб-сайт без перехода по ссылке.

Злоумышленники часто пытаются подтолкнуть вас к действию, поэтому с подозрением относитесь к любому веб-сайту, который просит вас действовать немедленно.

Это общие признаки фарминга. Если вы не уверены в веб-сайте, не вводите никакой информации. Для большей безопасности вы можете установить антифишинговую панель инструментов, которая предупредит вас, если вы находитесь на фишинговом веб-сайте.

5) Smishing: фишинговые атаки через SMS

Smishing — это фишинговая атака, в которой используются текстовые сообщения (SMS), чтобы обманным путем заставить пользователей выдать свою личную информацию.

Злоумышленники будут рассылать текстовые сообщения, которые выглядят как законные компании или организации. Текстовое сообщение обычно содержит ссылку на поддельный веб-сайт.

Пользователи, которые нажимают на ссылку, будут перенаправлены на поддельный веб-сайт, не осознавая этого. Поддельный веб-сайт будет выглядеть идентично реальному веб-сайту и иметь тот же бренд и логотип.

Однако URL-адрес будет немного другим. Например, фишинговый веб-сайт для Amazon может иметь URL-адрес, который выглядит следующим образом:

www.amazon.com.co.uk

Когда пользователи вводят свои учетные данные для входа на поддельный веб-сайт, злоумышленники украдут информацию об их учетной записи.

Как определить смишинг-атаки?

Смишинг-атаки может быть сложно идентифицировать, потому что текстовые сообщения выглядят идентично сообщениям легитимных компаний. Тем не менее, есть несколько красных флажков, на которые вы можете обратить внимание:

Будьте подозрительны, если вас просят щелкнуть ссылку в текстовом сообщении. Легальные компании редко будут просить вас сделать это.

Если текстовое сообщение отправлено высокопоставленным лицом, например, генеральным директором или финансовым директором, это может быть сокрушительной атакой.

Злоумышленники часто пытаются подтолкнуть вас к действию, поэтому с подозрением относитесь к любым текстовым сообщениям, в которых вас просят действовать немедленно.

Это общие индикаторы смишинг-атаки. Если вы не уверены в текстовом сообщении, не нажимайте никакие ссылки и не вводите никакой информации. Нет ничего плохого в том, чтобы связаться с компанией напрямую, чтобы проверить сообщение.

6) Вишинг: фишинговые атаки с помощью голосовых вызовов

Вишинг — это фишинговая атака, в которой используются голосовые вызовы (обычно через VoIP), чтобы обманным путем заставить пользователей выдать свою личную информацию.

Злоумышленники будут выдавать себя за законную компанию или организацию и называть жертву. Затем они попытаются обманом заставить жертву выдать личную информацию, например номер кредитной карты или номер социального страхования.

Как определить атаки вишинга?

Вишинг-атаки может быть сложно идентифицировать, потому что злоумышленник будет звучать как законный представитель компании или организации. Тем не менее, есть несколько красных флажков, на которые вы можете обратить внимание:

Если вас просят предоставить личную информацию, будьте подозрительны. Законные компании никогда не будут запрашивать такую информацию по телефону.

Если вас просят действовать немедленно, это может быть вишинг-атака. Злоумышленники часто пытаются подтолкнуть вас к действию.

Это общие индикаторы атаки вишинга. Попробуйте проверить личность звонящего, спросив его имя, отдел и контактную информацию. Если вы все еще не уверены, повесьте трубку и позвоните в компанию напрямую, чтобы проверить сообщение.

7) Клон-фишинг: атаки с использованием клонированных электронных писем.

Клон-фишинг — это тип фишинговой атаки, при которой используется клон законного электронного письма, чтобы обманным путем заставить пользователей выдать свою личную информацию.

Злоумышленник начнет с кражи законного электронного письма из почтового ящика жертвы. Затем они создадут клон электронного письма и изменят URL-адрес в сообщении на ссылку на поддельный веб-сайт.

Существует два типа фишинговых атак клонов:

1) злоумышленники могут создать копию оригинального письма и отправить его жертве

2) злоумышленники могут создать копию оригинального письма и отправить его контактам жертвы

Как идентифицировать фишинговые атаки-клоны?

Фишинговые атаки с клонированием могут быть сложными для выявления, поскольку они используют законную электронную почту, которая была клонирована. Тем не менее, есть несколько красных флажков, на которые вы можете обратить внимание:

Если вы получаете копию электронной почты, полученную ранее, это может быть фишинговой атакой клонирования.

Будьте подозрительны, если вас просят перейти по ссылке в электронном письме. Легальные компании редко будут просить вас сделать это.

Если электронное письмо отправлено высокопоставленным лицом, например генеральным директором или финансовым директором, это может быть клон фишинговой атаки.

Это общие признаки фишинговой атаки клонов. Если вы когда-либо не уверены в электронном письме, не нажимайте на ссылки и не вводите никакой информации. Нет ничего плохого в том, чтобы связаться с компанией напрямую, чтобы проверить сообщение.

8) Прогулки на снегоступах: спам с нескольких IP-адресов

Snowshoeing — это рассылка спама с использованием нескольких IP-адресов для отправки больших объемов электронной почты. Он получил свое название по аналогии со снегоступами, типом обуви, которая помогает распределять вес по большой площади.

Этот тип спама трудно обнаружить, поскольку он использует несколько IP-адресов, из-за чего создается впечатление, что электронные письма поступают из нескольких источников.

Как определить атаки на снегоступах?

Есть несколько индикаторов, по которым можно определить атаку на снегоступах:

Это может быть атака на снегоступах, если вы получаете большое количество писем от одного и того же отправителя.

Если электронные письма приходят с нескольких IP-адресов, это может быть атака на снегоступах.

Если электронные письма приходят с нескольких адресов, это может быть атака на снегоступах.

Это общие признаки нападения на снегоступах. Если вы думаете, что ходите на снегоступах, свяжитесь с компанией или организацией, которая предположительно отправляет электронные письма, чтобы проверить сообщение.

Вывод

Итак, вот некоторые из наиболее распространенных типов фишинговых атак. Обязательно следите за этими атаками и никогда не передавайте свою личную информацию кому-то, кого вы не знаете. Если вы считаете, что вас атакуют, свяжитесь с компанией или организацией, предположительно отправляющей электронные письма, чтобы проверить сообщение. Осведомленность о кибербезопасности — это непрерывный процесс информирования и обучения сотрудников угрозам, скрывающимся в киберпространстве». ***(Mahima Jaiswal. The Major Types of Phishing Attacks & How to Identify Them: The Definitive Guide // Techstrong Group Inc. (https://securityboulevard.com/2022/09/the-major-types-of-phishing-attacks-how-to-identify-them-the-definitive-guide/). 13.09.2022).***

***

«Новая фишинговая афера набирает обороты с конца июля, и эксперты по кибербезопасности немедленно предупреждают об этом.

Если вам случится получить странное электронное письмо, подтверждающее вашу верификацию в таком приложении, как Instagram, будьте осторожны, потому что вероятность того, что это мошенничество, невероятно высока.

Благодаря новому отчету VadeSecure, ведущей фирмы в области кибербезопасности, мы получили подробную информацию о мошенничестве, которое началось в июле 2022 года. Многие пользователи получают всевозможные электронные письма на одну и ту же тему.

Хакеры выдают себя за людей из Instagram, и это просто делает их невозможными для обнаружения, пояснил один из экспертов. Кроме того, электронное письмо также можно было увидеть, подтверждая, что профиль пользователя просматривается и утверждается для окончательной проверки.

В строке темы вы увидите заголовок, появится «информация о синем значке ig», а адрес электронной почты будет связан с «значками ig». Поначалу некоторым пользователям покажется, что электронное письмо очень настоящее и настоящее, поскольку можно увидеть оба логотипа Meta из Facebook и Instagram. Они отмечены на верхней и нижней части почты.

Эта умная тактика, используемая хакерами, является явным доказательством того, что они делают все, что в их силах, чтобы обмануть пользователя, заставив его думать, что это настолько реально, насколько это возможно. Но правда далека от этого, поскольку намерение не что иное, как злой умысел.

Но есть несколько замеченных орфографических ошибок и очень очевидных ошибок форматирования, для обнаружения которых не требуется специалист.

Фишинговая афера — это название, данное огромной проблеме, когда хакеры используют приманку, как в этом случае, когда есть шанс пройти проверку через Instagram. Таким образом, жертвы в конечном итоге щелкают вредоносные ссылки и вводят свои личные данные. И самое интересное, что мошенничество обычно происходит через электронные письма, и поэтому программное обеспечение безопасности не может блокировать или фильтровать их.

Инстаграм тоже прекрасно все это понимает. Недавно они упомянули в своем справочном центре, что весь процесс, связанный с проверкой, происходит через это приложение, а не через электронные письма. Следовательно, те, кто получает такие поддельные электронные письма, должны быть проинформированы о хакерах, стоящих за ними.

И запросы на верификацию применяются не ко всем. Вместо этого они предназначены для тех, кто включает знаменитостей, бренды или конкретных общественных деятелей. Следовательно, если и когда вы получаете такие вещи, лучше всего игнорировать их, а затем удалять». ***(Hura Anwar. Cybersecurity Experts Warn Against New Email Phishing Scam Where Hackers Pose As Instagram // Digital Information World (https://www.digitalinformationworld.com/2022/09/cybersecurity-experts-warn-against-new.html). 03.09.2022).***

***

«В последнее время вредоносное ПО Lampion распространяется в больших объемах, а злоумышленники злоупотребляют WeTransfer в рамках своих фишинговых кампаний.

WeTransfer — это законный сервис обмена файлами, которым можно пользоваться бесплатно, поэтому это бесплатный способ обойти программное обеспечение безопасности, которое может не вызывать предупреждений об URL-адресах, используемых в электронных письмах.

В рамках новой кампании, которую наблюдала фирма по обеспечению безопасности электронной почты Cofense, операторы Lampion рассылают фишинговые электронные письма со взломанных учетных записей компаний, призывая пользователей загрузить документ «Подтверждение платежа» с WeTransfer.

Файл, который получают цели, представляет собой ZIP-архив, содержащий файл VBS (Virtual Basic script), который жертва должна запустить для начала атаки.

После выполнения сценарий инициирует процесс WScript, который создает четыре файла VBS со случайными именами. Первый пустой, второй имеет минимальный функционал, а третий предназначен только для запуска четвертого скрипта.

Аналитики Cofense отмечают, что этот дополнительный шаг неясен, но модульные подходы к выполнению обычно предпочтительнее из-за их универсальности, позволяющей легко обмениваться файлами.

Четвертый сценарий запускает новый процесс WScript, который подключается к двум жестко заданным URL-адресам для извлечения двух DLL-файлов, спрятанных внутри защищенных паролем ZIP-файлов. URL-адреса указывают на экземпляры Amazon AWS.

Пароль для ZIP-файлов жестко запрограммирован в скрипте, поэтому архивы извлекаются без вмешательства пользователя. Содержащиеся полезные данные DLL загружаются в память, что позволяет скрытно запускать Lampion на скомпрометированных системах.

Оттуда Lampion начинает красть данные с компьютера, нацеливаясь на банковские счета, получая инъекции от C2 и накладывая свои собственные формы входа на страницы входа. Когда пользователи вводят свои учетные данные, эти поддельные формы входа будут украдены и отправлены злоумышленнику.

Троянская программа Lampion существует по крайней мере с 2019 года, ориентируясь в основном на испаноязычные цели и используя скомпрометированные серверы для размещения своих вредоносных ZIP-файлов.

В 2021 году Lampion впервые злоупотреблял облачными сервисами для размещения вредоносного ПО, включая Google Drive и pCloud.

Совсем недавно, в марте 2022 года, Cyware сообщила о всплеске распространения трояна, указав ссылку имени хоста на операции Bazaar и LockBit.

Cyware также сообщила, что авторы Lampion активно пытались усложнить анализ своего вредоносного ПО, добавляя дополнительные уровни обфускации и нежелательный код.

В последнем отчете Cofense указывается, что Lampion представляет собой активную и скрытую угрозу, и пользователям следует быть осторожными с нежелательными электронными письмами с просьбой загрузить файлы даже из законных облачных сервисов». ***(Bill Toulas. Lampion malware returns in phishing attacks abusing WeTransfer // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/lampion-malware-returns-in-phishing-attacks-abusing-wetransfer/). 09.09.2022).***

***

«Хакеры запускают новые атаки для кражи учетных данных Steam, используя метод фишинга «браузер в браузере», который становится все более популярным среди злоумышленников.

Техника «Браузер в браузере» — это популярный метод атаки, включающий создание фальшивых окон браузера в активном окне, что делает его всплывающей страницей входа для целевой службы входа.

В марте 2022 года BleepingComputer первым сообщил о возможностях этого нового фишингового комплекта, созданного исследователем безопасности mr.d0x. Используя этот фишинговый набор, злоумышленники создают поддельные формы входа в Steam, Microsoft, Google и любые другие сервисы.

Сегодня Group-IB опубликовала новый отчет по этой теме, иллюстрирующий, как новая кампания с использованием метода «Браузер в браузере» нацелена на пользователей Steam, преследуя аккаунты профессиональных геймеров.

Эти фишинговые атаки направлены на продажу доступа к этим учетным записям, при этом стоимость некоторых известных учетных записей Steam составляет от 100 000 до 300 000 долларов.

Group-IB сообщает, что фишинговый набор, использованный в наблюдаемой кампании Steam, не является широко доступным на хакерских форумах или в

даркнете. Вместо этого он используется в частном порядке хакерами, которые собираются вместе на каналах Discord или Telegram для координации своих атак.

Потенциальные жертвы получают прямые сообщения в Steam с приглашением присоединиться к команде для участия в турнирах по LoL, CS, Dota 2 или PUBG.

Ссылки, которыми делятся участники фишинга, приведут цели на фишинговый сайт, который, как представляется, является организацией, спонсирующей и проводящей киберспортивные соревнования.

Чтобы присоединиться к команде и принять участие в соревновании, посетителям предлагается войти в систему через свою учетную запись Steam. Однако новое окно страницы входа — это не настоящее окно браузера, наложенное поверх существующего веб-сайта, а поддельное окно, созданное на текущей странице, из-за чего его очень трудно распознать как фишинговую атаку.

Целевые страницы даже поддерживают 27 языков, определяя язык в настройках браузера жертвы и загружая правильный.

Как только жертва вводит свои учетные данные, новая форма предлагает ей ввести код 2FA. Если второй шаг не удался, отображается сообщение об ошибке.

Если аутентификация прошла успешно, пользователь перенаправляется на URL-адрес, указанный C2, обычно это законный адрес, чтобы свести к минимуму вероятность того, что жертва осознает компрометацию.

На данный момент учетные данные жертвы уже украдены и отправлены злоумышленникам. В подобных атаках злоумышленники быстро захватывают учетные записи Steam, меняя пароли и адреса электронной почты, чтобы жертвам было труднее восстановить контроль над своими учетными записями.

Во всех случаях фишинга «Браузер в браузере» URL-адрес в фишинговом окне является законным, поскольку злоумышленники могут отображать все, что захотят, поскольку это не окно браузера, а просто его рендеринг.

То же самое относится к символу блокировки SSL-сертификата, указывающему на HTTPS-соединение, что создает у жертв ложное чувство безопасности.

Хуже того, фишинговый комплект позволяет пользователям перетаскивать поддельное окно, сворачивать его, разворачивать и закрывать, что очень затрудняет обнаружение поддельного окна браузера в браузере.

Поскольку этот метод требует JavaScript, агрессивная блокировка JS-скриптов предотвратит отображение поддельного входа в систему. Однако большинство людей не блокируют скрипты, так как это нарушит работу многих популярных веб-сайтов.

Создатель инструментария Browser-in-the-Browser, Mr.D0x, сказал BleepingComputer, что лучший способ проверить, является ли всплывающее окно реальным, — попытаться переместить его за исходное окно браузера.

«Всегда старайтесь перетащить всплывающее окно к границе браузера. Если оно выходит за границы браузера, значит, это BiTB», — объясняет Mr.D0x.

Group-IB также поделилась следующими способами обнаружения атак типа «браузер в браузере»:

Проверьте, открывается ли новое окно на панели задач, если вы разгруппировали программы на панели задач Windows 10. Если нового окна панели

задач не существует, то это не настоящее окно. К сожалению, в настоящее время Windows 11 не поддерживает разгруппирование.

Попробуйте изменить размер окна. Если вы не можете это сделать, скорее всего, это поддельное окно браузера.

Поддельные окна браузера BiTB закроются, если вы свернете их.

В общем, будьте очень осторожны с прямыми сообщениями, полученными в Steam, Discord или других связанных с играми платформах, и избегайте переходов по ссылкам, отправленным пользователями, которых вы не знаете». ***(Bill Toulas. Hackers steal Steam accounts in new Browser-in-the-Browser attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-steal-steam-accounts-in-new-browser-in-the-browser-attacks/). 12.09.2022).***

***

«Злоумышленники используют смерть королевы Елизаветы II в фишинговых атаках, чтобы заманить своих жертв на сайты, которые крадут учетные данные их учетных записей Microsoft.

Помимо данных учетной записи Microsoft, злоумышленники также пытаются украсть коды многофакторной аутентификации (MFA) своих жертв, чтобы завладеть их учетными записями.

«Сообщения якобы исходили от Microsoft и приглашали получателей посетить «центр искусственных технологий» в ее честь», — сообщила сегодня команда Proofpoint Threat Insight.

В кампании, обнаруженной Proofpoint, мошенники выдавали себя за «команду Microsoft» и пытались заставить получателей добавить свои заметки на онлайн-доску памяти «в память о Ее Величестве королеве Елизавете II».

После нажатия кнопки, встроенной в фишинговое электронное письмо, цели вместо этого отправляются на фишинговую целевую страницу, где их сначала просят ввести свои учетные данные Microsoft.

«Сообщения содержали ссылки на URL-адрес, перенаправляющий страницу сбора учетных данных, нацеленную на учетные данные электронной почты Microsoft, включая коллекцию MFA», — добавил Proofpoint.

Злоумышленники используют новую платформу Phishing-as-a-Service (PaaS) с обратным прокси-сервером, известную как EvilProxy, продвигаемую на хакерских форумах в чистой сети и даркнете, которая позволяет злоумышленникам с низким уровнем квалификации красть токены аутентификации для обхода MFA.

Национальный центр кибербезопасности Соединенного Королевства предупредил во вторник о повышенном риске использования киберпреступниками смерти королевы в своих целях в фишинговых кампаниях и других видах мошенничества.

«Хотя NCSC, который является частью GCHQ, еще не видел подробных доказательств этого, как всегда, вы должны знать, что это возможно, и внимательно относиться к электронным письмам, текстовым сообщениям и другим сообщениям, касающимся смерти Ее Величества. Queen и приготовления к ее похоронам», — говорится в сообщении NCSC.

Хотя эта вредоносная деятельность кажется ограниченной, NCSC зафиксировал такие фишинговые атаки и в настоящее время расследует их.

Источники также сообщили BleepingComputer, что NCSC известно о фишинговых сообщениях, в которых злоумышленники пытаются обманом заставить потенциальных жертв передать конфиденциальную информацию, включая банковские реквизиты.

«Киберпреступники часто играют на ваших эмоциях, чтобы заставить вас кликнуть, а также могут ссылаться на громкие текущие события», — добавило агентство.

«Часто цель состоит в том, чтобы заставить вас посетить веб-сайт, который может загрузить вирус на ваш компьютер или украсть банковские реквизиты или другую личную информацию». ***(Sergiu Gatlan. Death of Queen Elizabeth II exploited to steal Microsoft credentials // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/death-of-queen-elizabeth-ii-exploited-to-steal-microsoft-credentials/). 14.09.2022).***

***

Технічні аспекти кібербезпеки

«…До недавнего времени большинство компаний не знали об «ингредиентах» или коде, из которых состоит программное обеспечение, лежащее в основе их продуктов и корпоративного программного обеспечения. Это проблема, потому что использование стороннего кода растет, а потребление программного обеспечения с открытым исходным кодом (OSS) ускорится в ближайшие годы.

Компании используют OSS, потому что это снижает затраты и ускоряет разработку программного обеспечения. Наслаивая код, который уже создан кем-то другим, разработчики могут сократить время выхода на рынок и ускорить наборы функций, наиболее востребованные их деловыми партнерами. Проблема заключается в том, что код в репозитории OSS может содержать встроенные вредоносные программы, ошибки или другие уязвимости, о которых разработчик не знает. Без надежного процесса проверки кода в репозитории OSS, из которого их разработчики извлекают данные, компании не будут знать об угрозах, таящихся в их продуктах.

Чтобы идти в ногу с меняющейся динамикой безопасности, компаниям нужны новые программы и методы управления, чтобы понять происхождение и безопасность кода, лежащего в основе их цифровых продуктов и бизнес-операций. Без такой системы компании останутся уязвимыми для непреднамеренной установки вредоносных программ, которые могут вызвать инциденты кибербезопасности или повредить важные приложения. Хотя некоторых киберугроз можно избежать, разработав собственный код собственными силами, этот процесс требует больших ресурсов и времени. Кроме того, использование OSS имеет такие преимущества, как возможность быстрого создания в облаке или повышение производительности труда разработчиков. На самом деле большинство приложений

создаются с использованием комбинации пользовательского кода и компонентов с открытым исходным кодом. Именно тогда деликатное уравновешивание ложится на главных технических директоров (CTO), директоров по информационным технологиям (CIO).

Чтобы идти в ногу с меняющейся динамикой безопасности, компаниям нужны новые программы и методы управления, чтобы понять происхождение и безопасность кода, лежащего в основе их цифровых продуктов и бизнес-операций.

Программа спецификации программного обеспечения (SBOM) может помочь компаниям защитить себя и своих клиентов, создав систему, которая проверяет весь входящий код, прежде чем он может быть принят разработчиками.

Что такое SBOM и почему это помогает

SBOM похож на этикетку пищевой ценности на коробке с хлопьями: в нем перечислены ингредиенты внутри, выделено содержание, которое может быть вредным для некоторых, например, глютен и арахис. В частности, SBOM представляет собой формальный машиночитаемый перечень программных компонентов и зависимостей (которые являются результатом объединения различных компонентов OSS, стороннего кода и кода, разработанного внутри компании), технической информации об этих компонентах и иерархических связях кода…

SBOM помогает разработчикам узнать происхождение «кода за кодом», чтобы они могли определить, является ли он безопасным. Это также помогает им понять и устранить известные уязвимости в коде, экономя время и деньги. SBOM также помогают юридическим отделам и отделам соблюдения нормативных требований определить историю лицензий и допустимые варианты использования фрагмента стороннего кода, что снижает вероятность любого неправомерного использования. Кроме того, SBOM помогают специалистам по безопасности и криминалистике определить воздействие на программное обеспечение после обнаружения вновь выявленных распространенных уязвимостей и рисков (CVE), что повышает способность организаций реагировать и устранять уязвимости.

Зачем нужна программа SBOM

За последние пять лет разработка OSS выросла примерно с 35 процентов до примерно 75 процентов проверенной кодовой базы организаций.1 Например, к 2021 году, по данным OpenUK, девять из десяти британских компаний сообщили об использовании OSS.2 Организации используют OSS, потому что это способствует экономии средств, гибкости разработчиков и скорости кодирования.

Использование OSS создает возможности для более тесного сотрудничества с разработчиками и позволяет программистам быстро двигаться вперед, поскольку библиотеки кода содержат неограниченное количество готовых функций и инструментальных ресурсов. Наличие программных компонентов, доступных по запросу, позволяет разработчикам использовать результаты работы других разработчиков. Компоненты доступны и доступны из любого места, и эти элементы не зависят от отдельных производителей, что делает их привлекательными для стартапов и новых игроков в области технологий — или, по сути, для всех, кто хочет быстро создавать программное обеспечение.

Хотя преимущества использования стороннего кода очевидны, OSS вносит свой вклад в организационные риски. OSS не регулируется и не контролируется центральным органом и является общедоступным. Он может содержать потенциальные уязвимости, устаревший код и киберэксплойты, которые могут подвергать организации кибератакам. Большинство организаций стремятся лучше понять и снизить свои кибер- и технологические риски, но организации признают, что создание и поддержка безопасного кода является жизненно важным краеугольным камнем любой стратегии кибербезопасности.

Организации больше не задаются вопросом, пострадают ли они от кибератаки, а вместо этого спрашивают, когда, как и какое воздействие будет после кибератаки. В 2014 году 62% организаций сообщили о кибератаках. К 2021 году это число выросло до 86 процентов. Стоимость кибератак также быстро растет. Согласно отчету Verizon о расследовании нарушений данных, в 2015 году глобальное воздействие киберпреступности оценивалось в 3 триллиона долларов. К 2021 году эта цифра увеличится примерно до 6 трлн долларов, а к 2025 году ожидается рост примерно до 10 трлн долларов. Из тысяч ежедневных кибератак все чаще причиной становятся уязвимости цепочки поставок.

Учитывая преимущества OSS, а также связанные с ним риски, компаниям становится все труднее управлять своими цепочками поставок программного обеспечения. Например, в декабре 2020 года выяснилось, что эксплойт вредоносного ПО Sunburst имеет происхождение из цепочки поставок. Инцидент затронул около 33 000 пользователей, 18 000 из которых заразили продукт вредоносным кодом.

SBOM позволяют компаниям сохранить преимущества OSS, управляя рисками. Они помогают компаниям предотвращать проблемы, как в случае с Sunburst, когда одна компания, у которой была возможность SBOM, смогла определить, что она уязвима для зараженного кода, в течение двух часов. Другим пострадавшим повезло меньше, например, энергетической компании, которая два с половиной месяца спустя определила, что у нее плохое программное обеспечение. В течение этих двух с половиной месяцев компания была уязвима для еще большего количества атак и компрометации предприятия.

Киберпреступники и другие злоумышленники часто используют различные методы для запуска атак на цепочку поставок программного обеспечения, часто нацеленных на код с открытым исходным кодом или распространенный сторонний код. С этой целью в 2018 году исследователи обнаружили 12 вредоносных библиотек Python, загруженных в официальный индекс пакетов Python (PyPI).3 В совокупности такие инциденты, как случай с вредоносным ПО Sunburst и компрометация индекса пакетов Python, побудили компании задуматься о быстрой разработке SBOM (см. врезку «Федеральное правительство хочет защитить страну от вредоносного кода»).

Как программы SBOM снижают риски за счет повышения прозрачности кода

В большинстве организаций есть приложения, состоящие из различных подкомпонентов и частей, некоторые из которых взяты из библиотек OSS, другие приобретены у третьих лиц, а некоторые созданы и настроены разработчиками. Каждый источник имеет различные ограничения, связанные с ним. Например, OSS и стороннее программное обеспечение имеют лицензии, которые со временем

меняются или могут иметь ограничения на использование. Типичная система SBOM исследует, идентифицирует и характеризует эти элементы кодирования…

Организации, которые изо всех сил пытаются понять уязвимости в своем коде, подвергают себя риску безопасности или финансам. Вот несколько преимуществ, которые организация может получить от создания программы SBOM:

Выявление уязвимостей и их устранение. Системы SBOM инвентаризируют подкомпоненты кода и позволяют аналитикам идентифицировать код с известными уязвимостями. Когда объявляется о критической уязвимости, аналитики безопасности обращаются к артефактам SBOM и определяют, есть ли влияние на код. Это помогает персоналу реагирования на инциденты определить, где существуют уязвимости, и расставить приоритеты по их устранению. Он также дает руководителям возможность быстро и уверенно реагировать на запросы членов совета директоров, клиентов, инвесторов и регулирующих органов.

Управление лицензиями на программное обеспечение. Программы SBOM помогают организациям управлять своим сторонним программным обеспечением и лицензиями OSS, которые могут быть довольно сложными и меняться со временем. Это гарантирует, что разработчики смогут постоянно определять допустимые варианты использования OSS и стороннего программного обеспечения, в конечном итоге защищая организации от финансовых рисков, связанных с ненадлежащим или несанкционированным использованием стороннего программного обеспечения. Это также помогает командам по обеспечению соответствия требованиям реагировать на претензии по поводу лицензий или аудиты.

Улучшение жизненного цикла разработки программного обеспечения (SDLC). Программы SBOM могут помочь организациям улучшить свои SDLC. Создание SBOM в заданное время во время SDLC может выявить такие проблемы, как известные уязвимости или проблемы с лицензией. Команды устраняют эти проблемы на раннем этапе, сокращая расходы и предотвращая задержки. Программы SBOM позволяют организациям стать более эффективными и ускорить создание, развертывание и запуск программного обеспечения.

Например, по мере создания кода разработчики создают начальный SBOM, в котором перечислены зависимости, присущие программному обеспечению. Во время тестирования и упаковки выявляются уязвимости и дополнительные зависимости, а SBOM обновляется по мере развертывания кода. По мере появления уязвимостей во время работы программа SBOM будет предупреждать разработчиков о необходимости исправления. После исправления SBOM снова обновляется.

Как разработать программу SBOM: инвестировать, создавать, интегрировать и проектировать

Осознавая преимущества и проблемы, связанные с разработкой OSS, становится ясно, что программы SBOM являются неотъемлемой частью более безопасного кодирования и устойчивости предприятия. С этой целью организации могут сосредоточиться на четырех ключевых методах при создании программ SBOM:

Инвестируйте в возможности SBOM, опираясь на существующие инструменты анализа состава программного обеспечения (SCA). Во многих организациях есть возможности SCA. В зависимости от того, насколько надежны

возможности, команды могут использовать это в качестве основы для создания программы SBOM. Руководство может эффективно использовать ресурсы, определяя, какие инструменты SBOM можно приобрести, а какие разрабатывать самостоятельно. Руководители продуктов должны найти надежного поставщика и создать программу с использованием инструментов, соответствующих процессам SDLC, включая плавную и автоматизированную интеграцию с конвейером непрерывной интеграции и непрерывного развертывания (CI/CD). Автоматизированные возможности SBOM могут быть разработаны собственными силами или приобретены у стороннего поставщика.

Создайте программу SBOM с межфункциональной командой. Программы SBOM включают несколько частей организации, каждая из которых играет свою роль. Важно запустить программу SBOM, используя кросс-функциональную команду. В эту команду должны входить сотрудники с различным опытом — разработчики, информационная безопасность, закупки, юриспруденция, управление рисками, конфиденциальность и соблюдение нормативных требований, поскольку программы SBOM затрагивают несколько частей организации. Каждая участвующая команда должна быть представлена на уровне принятия решений, и их потребности должны учитываться на протяжении всего процесса (Иллюстрация 3).

Интегрируйте SBOM в SDLC. Программы SBOM обеспечивают преимущества для разработчиков, выявляя уязвимости и проблемы с лицензированием на ранних этапах процесса. Организации могут получить наибольшую выгоду, если они изучат свои процессы разработки и интегрируют создание и проверку SBOM на нескольких этапах жизненного цикла разработки. Создание автоматизированных возможностей создания и проверки SBOM снижает рабочую нагрузку и побуждает разработчиков внедрять новые способы работы.

Управление дизайном СБОМ. Программы SBOM требуют межфункционального сотрудничества и коммуникации и могут потребовать дополнительной структуры для стимулирования принятия, соблюдения и сотрудничества. Организациям с децентрализованной или неиерархической культурой может быть сложно заставить разработчиков соблюдать требования SBOM. Преимущества безопасности и эффективность SDLC помогают повысить заинтересованность разработчиков. Кроме того, организации могут рассмотреть структуру управления, в которой распределяются роли и обязанности для задач, связанных с SBOM…

Запуск программы SBOM

Компании стремятся использовать сторонний код, включая OSS, а это означает, что создание программы SBOM должно соответствовать их примеру, чтобы избежать проблем, с которыми сегодня сталкиваются многие в деловом мире. В дополнение к этой статье руководство по созданию программы доступно на форумах разработчиков Агентства кибербезопасности и безопасности инфраструктуры (CISA) и Национального института стандартов и технологий (NIST).4 Правила SBOM в первую очередь касаются компаний, предоставляющих услуги правительству, таких как аэрокосмическая и оборонная промышленность, но они могут быть полезным руководством для всех компаний, стремящихся смягчить те же проблемы. Строго регулируемые отрасли, такие как коммунальные услуги и

финансовые услуги, часто несут такую же ответственность за мониторинг использования программного обеспечения OSS.

Забегая вперед, организации, которые заранее изучают и оценивают код, который входит в их экосистему с помощью надежной программы SBOM, будут лучше подготовлены к предстоящим правительственным постановлениям о цепочке поставок программного обеспечения и обеспечат безопасность своей ИТ-инфраструктуры и клиентов. Надежные программы SBOM позволяют организациям экономично и эффективно создавать безопасный код перед лицом растущих киберугроз. Настало время действовать сейчас». ***(Tucker Bailey, Justin Greis, Matt Watters, and Josh Welle. Software bill of materials: Managing software cybersecurity risks // McKinsey & Company (https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/software-bill-of-materials-managing-software-cybersecurity-risks). 19.09.2022).***

***

«Агентство кибербезопасности и безопасности инфраструктуры (CISA) и Агентство национальной безопасности (АНБ) через Enduring Security Framework (ESF) опубликовали документ под названием «Соображения безопасности сети открытого радиодоступа», в котором оцениваются преимущества и соображения безопасности при внедрении архитектуры Open RAN.

Рабочая группа ESF Open RAN сосредоточила внимание на соображениях безопасности для нескольких ключевых технических аспектов Open RAN: управление несколькими поставщиками, Open Fronthaul, соединяющий радиостанции с оборудованием базовой станции, новая структура приложений RAN, включающая rApps и xApps, использование искусственного интеллекта. Машинное обучение (AI/ML) для оптимизации RAN и других общих аспектов сети, включая программное обеспечение с открытым исходным кодом, виртуализацию и облачную базовую сеть 5G.

«Соображения безопасности всегда возникают в новых открытых системах, направленных на повышение стоимости, производительности и преимуществ цепочки поставок», — сказал Хорхе Лорел, директор проекта ESF. «Open RAN также разделяет эти соображения безопасности, и благодаря постоянным усилиям экосистемы Open RAN их можно преодолеть».

«Открытая RAN — это захватывающая концепция, которая открывает несколько дверей для инноваций, повышения производительности сети и создания более разнообразной и конкурентоспособной киберэкосистемы», — сказала исполняющая обязанности помощника директора CISA Мона Харрингтон. «Однако вместе с этими преимуществами возникают дополнительные проблемы с безопасностью. Как сообщество, мы должны работать вместе, чтобы не только выявить эти проблемы, но и разработать методы и архитектуру для их смягчения»... ***(SECURING 5G OPEN RAN ARCHITECTURE FROM CYBERSECURITY RISKS // Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/blog/2022/09/15/securing-5g-open-ran-architecture-cybersecurity-risks). 15.09.2022).***

***

«API или интерфейс прикладного программирования — это де-факто строительный блок для современных приложений, необходимый как для создания, так и для подключения приложений и веб-сайтов. Но API плохо защищены и стали одной из основных целей для атак, особенно атак ботов.

По данным perimeterx, 75% попыток входа в систему с конечных точек API (интерфейсов прикладного программирования) являются вредоносными. Хакеры систематически используют ботов для злонамеренных попыток входа в систему.

Как вы можете защитить свои API от ботов и бот-атак? Продолжайте читать, чтобы узнать об эффективных способах обнаружения и защиты API-ботов.

Почему API подвержены риску атак ботов?

API-интерфейсы позволяют разработчикам с большей легкостью получать доступ, повторно использовать и интегрировать функциональные активы и данные, обеспечивая гибкость, скорость и эффективность разработки. Это привело к увеличению зависимости от API со стороны организаций, которые в настоящее время развертывают все больше и больше таких интерфейсов, чтобы помочь своим инициативам в области цифровой трансформации. Тем не менее, API-интерфейсы часто подвержены риску кибератак ботов, таких как DoS- и DDoS-атаки, атаки с скрейпингом контента и ценообразования, захват учетных записей и т. д.

В 2020 году 98 % организаций столкнулись с атаками на свои приложения/веб-сайты, а 82 % сообщили, что это были кибератаки ботов. Несколько организаций ежемесячно сталкиваются как минимум с одной DoS/DDoS-атакой или какой-либо формой внедрения или манипулирования атрибутами.

Почему риск кибератак ботов на API настолько высок и распространен?

40% организаций сообщили, что более половины их приложений доступны сторонним службам или Интернету благодаря API.

Атаки API с использованием ботов легче организовать, поскольку ботнеты легко доступны для аренды.

Традиционные методы обнаружения и предотвращения, такие как ограничение скорости, обнаружение на основе сигнатур, протоколы блокировки и т. д., оказались недостаточными для защиты от очень сложных атак ботов API.

Злоумышленники используют. Организациям трудно провести различие между действиями людей и ботов, а также между хорошими и плохими ботами, что серьезно ограничивает их возможности по защите API от атак ботов.

Запросы API не проходят через традиционный маршрут браузеров или собственных агентов приложений; они служат прямым конвейером с доступом к ресурсам и функциям. Это делает API прибыльными целями для злоумышленников.

Часто разработчики используют стандартные/общие наборы правил для API, не помня о бизнес-логике. Это открывает API для уязвимостей бизнес-логики, которые часто используются с помощью ботов для разрушения.

Как защитить свои API от атак ботов?

Соберите разведданные и создайте основу для нормального поведения

Чтобы эффективно защитить API от ботов, вам необходимо установить, что является приемлемым, нормальным поведением, а что — аномальным поведением.

С этой целью ваше решение по обеспечению безопасности должно отслеживать трафик API и собирать информацию с помощью снятия отпечатков пальцев, поведенческого анализа, анализа шаблонов и эвристического анализа, проверки рабочего процесса, глобальных каналов угроз, времени отклика сети и т. д. построить основу того, что считается поведением людей и ботов, а в поведении ботов — хорошим и плохим поведением.

Этот процесс должен быть непрерывным, поскольку цифровой ландшафт быстро развивается; Злоумышленники постоянно используют сложные технологии, чтобы боты могли имитировать поведение человека. Вам необходимо постоянно пересматривать приемлемое и вредоносное поведение в отношении безопасности API.

Постоянно отслеживать запросы API

Детально отслеживайте все запросы API в соответствии с базовой моделью. Процесс обнаружения ботов в API должен быть интеллектуальным (с использованием самообучающегося ИИ, глубокой аналитики и автоматизации) и гибким, чтобы обеспечить гибкость, скорость и точность обнаружения активности ботов в реальном времени. Непрерывный мониторинг и регистрация одинаково важны.

Разверните методы мгновенного устранения плохих ботов

Чтобы защитить API от ботов, нельзя останавливаться на обнаружении в реальном времени; вы должны иметь возможность блокировать доступ вредоносных ботов к API и критически важным ресурсам, которые API часто раскрывают. С этой целью интеллектуальные решения для управления ботами API работают мгновенно и разумно против самых сложных и скрытных вредоносных ботов.

Интеллектуальные инструменты управления ботами API определяют, следует ли разрешать, блокировать, помечать или оспаривать входящие запросы API, на основе информации и сигналов в реальном времени. В сочетании с надежной системой контроля ложных срабатываний это помогает свести к минимуму ложноположительные и ложноотрицательные результаты. Другими словами, они создают препятствия для доступа плохих ботов и злоумышленников к API, а не к легитимному трафику и к хорошим ботам.

Внедрение архитектур с нулевым доверием

Внедрите архитектуру с нулевым доверием, в которой каждый пользователь должен подтвердить свою личность и получить доступ на основе своей роли и только в той степени, в которой это необходимо для выполнения необходимых действий. Неограниченные, непроверенные разрешения и привилегии наносят ущерб безопасности API, особенно против кибератак ботов, таких как подстановка учетных данных и атаки грубой силы. Внедрите надежные средства управления доступом на основе ролей, надежные политики паролей и многофакторную аутентификацию.

Настройка наборов правил

Адаптируйте свои наборы правил на основе контекстной аналитики, чтобы предотвратить использование недостатков бизнес-логики и других уязвимостей в API ботами. Кроме того, заручитесь помощью сертифицированных экспертов по безопасности для точного создания политик безопасности.

Вывод

Чтобы эффективно защитить API от атак ботов, используйте AppTrana API Protection — передовое комплексное решение для защиты API с учетом рисков. Он обеспечивает защиту от ботов для ваших API с помощью позитивных политик безопасности, ботов, специфичных для API, и политик смягчения DDoS». ***(Vinugayathri Chinnasamy. Bad bots are coming at APIs! How to beat the API bot attacks? // Help Net Security (https://www.helpnetsecurity.com/2022/09/12/api-bot-attacks/). 12.09.2022).***

***

«Исследователи безопасности разработали реализацию утилиты Sysinternals PsExec, которая позволяет перемещаться по сети с использованием одного менее контролируемого порта Windows TCP 135.

PsExec предназначен для того, чтобы помочь администраторам удаленно выполнять процессы на компьютерах в сети без необходимости установки клиента.

Злоумышленники также внедрили этот инструмент и часто используют его на постэксплуатационных этапах атаки для распространения по сети, выполнения команд в нескольких системах или развертывания вредоносных программ.

В то время как оригинальный PsExec доступен в наборе утилит Sysinternals, в коллекции Impacket также есть реализация классов Python для работы с сетевыми протоколами, которая имеет поддержку SMB и других протоколов, таких как IP, UDP, TCP, которые разрешают соединения для HTTP, LDAP (облегченный протокол доступа к каталогам) и Microsoft SQL Server (MSSQL).

И оригинальная версия, и вариант Impacket работают одинаково. Они используют соединение SMB и основаны на порте 445, который должен быть открыт для обмена данными по сетевому протоколу обмена файлами SMB.

Они также управляют службами Windows (создают, выполняют, запускают, останавливают) с помощью удаленных вызовов процедур (RPC) — протокола, обеспечивающего высокоуровневую связь с операционной системой.

Однако для расширенной функциональности требуется порт 135. Однако блокировка этого порта не мешает злоумышленнику завершить атаку, поэтому порт 445 необходим для работы PsExec.

Из-за этого защитники в основном сосредотачиваются на блокировке порта 445, который необходим PsExec для выполнения команд или запуска файлов. Это работает в большинстве случаев, но этого недостаточно.

Новая реализация PsExec

На основе библиотеки Impacket исследователи из Pentera, компании, которая предоставляет решение для автоматической проверки безопасности, создали реализацию инструмента PsExec, который работает только на порту 135.

Это достижение вносит изменения в игру защиты, поскольку блокировка только порта 445 для ограничения вредоносной активности PsExec больше не является надежным вариантом для большинства атак.

«Мы обнаружили, что протокол SMB используется для загрузки двоичного файла и перенаправления ввода и вывода», — объясняет Юваль Лазар, старший исследователь безопасности в Pentera.

Лазар добавляет в отчет, предоставленный BleepingComputer, что команды выполняются через распределенную вычислительную среду / удаленные вызовы процедур (DCE / RPC), а процессы «запускаются независимо от вывода».

Разновидность PsExec от Pentera использует соединение RPC, что позволило исследователям создать службу, которая запускает произвольную команду без связи через порт 445 SMB для передачи или вывода.

В отличие от оригинального PsExec в пакете Sysinternals, у варианта Pentera больше шансов остаться незамеченным в сети, сказал Лазар BleepingComputer, потому что многие организации следят за портом 445 и SMB.

Еще один момент, на который указывает Лазар, заключается в том, что другие реализации PsExec должны использовать SMB, поскольку они основаны на файлах. По словам исследователя, вариант Pentera не содержит файлов, что затрудняет его обнаружение.

Исследование Лазара, посвященное PsExec, показывает, что хотя такие уязвимости безопасности, как PetitPotam [1, 2] и DFSCoerce, привлекли внимание к рискам, которые представляет RPC, меры по их устранению сосредоточены не на мониторинге DCE/RPC, а на предотвращении ретрансляции NTLM.

По наблюдениям Pentera, блокировка или мониторинг RPC-трафика не является обычной практикой в корпоративной среде. Причина во многих случаях заключается в том, что защитники не знают, что RPC может представлять угрозу безопасности сети, если его не остановить.

Уилл Дорманн, аналитик по уязвимостям в CERT/CC, согласен с тем, что одной блокировки TCP-порта 445 недостаточно, чтобы заблокировать вредоносную активность, основанную на этом инструменте.

«Если люди думают, что блокировки только 445 достаточно для предотвращения PsExec (и других вещей, связанных с RPC), то они ошибаются», — сказал исследователь BleepingComputer.

PsExec основан на соединениях SMB и RPC, для которых требуются порты 445, 139 и 135. Однако Лазар добавил, что существует реализация RPC поверх HTTP, а это означает, что PsExec потенциально может работать и через порт 80.

PsExec популярен среди хакеров-вымогателей

Хакеры уже давно используют PsExec в своих атаках. Банды вымогателей, в частности, использовали его для развертывания вредоносного ПО для шифрования файлов.

В атаке, которая длилась всего один час, программа-вымогатель NetWalker использовала PsExec для запуска своей полезной нагрузки на всех системах в домене.

В более свежем примере банда вымогателей Quantum полагалась на PsExec и WMI для шифрования систем в атаке, которая заняла всего два часа после получения доступа через вредоносное ПО IcedID.

В июньском отчете Microsoft подробно описывается атака программы-вымогателя BlackCat, которая также использовала PsExec для распространения полезной нагрузки программы-вымогателя.

Другим примером является недавно обнаруженная брешь в Cisco, когда банда вымогателей Yanluowang использовала PsExec для удаленного добавления значений

реестра, что позволило злоумышленнику использовать функции специальных возможностей, доступные на экране входа в систему Windows». ***(Ionut Ilascu. New PsExec spinoff lets hackers bypass network security defenses // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-psexec-spinoff-lets-hackers-bypass-network-security-defenses/). 13.09.2022).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«В США ФБР обнаружило сотни уязвимостей в медицинских устройствах после недавних предупреждений Агентства кибербезопасности и безопасности инфраструктуры (CISA). Эти медицинские устройства, в том числе инсулиновые помпы, внутрисердечные дефибрилляторы, мобильные кардиотелеметры, кардиостимуляторы и интратекальные обезболивающие помпы, слишком часто работают на устаревшем программном обеспечении и не имеют адекватных функций безопасности.

Например, CISA выявила уязвимости в мониторе пациента Contec Health CMS8000 Vital Signs. Это устройство предназначено для мониторинга частоты сердечных сокращений пациента, насыщения кислородом, температуры и других показателей жизнедеятельности.

В результате хакеры могут завладеть устройствами и изменить показания, ввести передозировку наркотиков и угрожать здоровью пациентов.

Чтобы лучше понять риски, Digital Journal связалась с Салли Винсент, старшим инженером по исследованию угроз в LogRhythm…

Обращая внимание на медицинские устройства, Винсент обнаруживает: «ФБР недавно обнаружило сотни уязвимостей в медицинских устройствах, таких как инсулиновые помпы, внутрисердечные дефибрилляторы, мобильные кардиотелеметры, кардиостимуляторы и интратекальные обезболивающие насосы».

Проблема в том, что по мере развития большинства технологий многие программы, управляющие медицинскими устройствами или собирающие информацию, оставались неизменными. Здесь Винсент отмечает: «Многим из этих устройств уже более 30 лет, на них установлено устаревшее программное обеспечение и отсутствуют адекватные функции безопасности».

Это приводит к рискам, которые Винсент резюмирует следующим образом: «Эти результаты проливают свет на потенциальные опасности неадекватности безопасности в секторе здравоохранения, включая угрозы для доверия к медицинским организациям и, что более важно, для жизни и данных пациентов».

Риски принимают и другие формы. По словам Винсента: «Стоимость кибератаки является самой высокой в сфере здравоохранения, поэтому организациям здравоохранения крайне важно держать средства контроля кибербезопасности в центре внимания — инвестиции в более современные медицинские устройства — это только первый шаг».

Чтобы исправить это, необходимо принять меры. Винсент рекомендует: «Организациям важно принять конкретные меры кибербезопасности для обеспечения безопасности своих пациентов, в том числе усовершенствовать свои планы реагирования на инциденты, чтобы быстро и эффективно смягчить последствия взлома».

Винсент также советует: «Организации здравоохранения также должны внедрить гигиену паролей, возможности обнаружения угроз и меры превентивного реагирования и реагирования, которые могут помешать злонамеренным киберпреступникам, защитить данные пациентов и обеспечить бесперебойную работу повседневных процессов ИТ-систем».

Винсент отмечает, что, следуя этому совету, можно добиться успеха: «Благодаря этим изменениям организации здравоохранения получат полную информацию о своей ИТ-среде, что в конечном итоге позволит лучше защитить своих пациентов и сохранить в безопасности ценные данные». ***(Tim Sandle. Alert issued over cybersecurity concerns in hundreds of medical devices // DIGITAL JOURNAL INC. (https://www.digitaljournal.com/tech-science/alert-issued-over-cybersecurity-concerns-in-hundreds-of-medical-devices/article). 19.09.2022).***

***

«Как показал опрос BlueVoyant, безопасному производству, распространению и управлению медиафайлами угрожает сложная, фрагментированная сторонняя экосистема, в результате чего медиа-индустрия подвергается потенциальным угрозам кибербезопасности.

Отчет показал, что 30% поставщиков средств массовой информации подвержены компрометации из-за уязвимостей, обнаруженных в их общедоступных интернет-сайтах. Процент медиа-вендоров, подверженных компрометации, в два раза выше, чем в межотраслевом эталонном тесте, составленном из всех компаний, мониторы которых BlueVoyant.

Опрос показал, что половина ведущих поставщиков медиа, предоставляющих решения для управления контентом (CMS), имеют потенциально компрометирующие уязвимости, и своевременное исправление также является серьезной проблемой. Целых 60% выявленных уязвимых систем остаются незащищенными через шесть недель после выпуска исправления.

«В результате обнаруженных нами уязвимостей медиа-компании могут быть уязвимы для кибератак, включая программы-вымогатели и сбои в работе», — сказал Джоэл Молинофф, вице-председатель BlueVoyant. «Известно, что обнаруженные нами критические уязвимости могут быть использованы злоумышленниками, поэтому угрозы вполне реальны. Эти уязвимости также могут привести к утечке контента».

Он указал, что предварительный выпуск контента часто передается поддерживающим поставщикам в рамках производственного процесса, и если один из этих поставщиков будет скомпрометирован, контент может просочиться до его запланированного выпуска.

«Медиаиндустрия полагается на поставщиков для производства контента и выпуска нового контента для потребителей», — пояснил Молинофф. «В целом, по

мере того, как внутренние сети компаний становятся все более защищенными, часто третья сторона, например продавец или поставщик, становится слабым звеном. У многих медиакомпаний сотни, если не тысячи поставщиков, поэтому следить за ними непросто».

Кроме того, большинство поставщиков медиа-индустрии являются относительно небольшими компаниями, у которых нет ни соответствующего бюджета на кибербезопасность, ни необходимого внимания к рискам кибербезопасности.

Кибербезопасность не является приоритетом СМИ

Он добавил, что еще одной проблемой для отрасли является ее зависимость от устаревших систем.

«Цепочки создания стоимости в СМИ были разработаны давно и зависят от лежащих в их основе технологий, — сказал он. «Внедрение новых, более безопасных технологий происходит медленно из-за стоимости и возможных сбоев».

Майк Паркин, старший технический инженер Vulcan Cyber, поставщика SaaS для устранения рисков корпоративной кибербезопасности, сказал, что кибербезопасность не является главным приоритетом во многих отраслях, включая СМИ.

«Многие организации полагаются на обширную экосистему для ведения бизнеса, и медиа-компании не являются исключением», — сказал он. «Учитывая широкий спектр функций, доступных на медиа-сайтах, часто разработанных сторонними организациями, неудивительно, что существует проблема обеспечения их безопасности».

С точки зрения Паркина, медиа-компании, как и любая организация, должны требовать от своих сторонних поставщиков и поставщиков более высоких стандартов, чтобы убедиться, что они предоставляют услуги, которые должным образом защищены, и защищают свою собственную среду.

Им также необходимо разобраться в своей среде и убедиться, что у них есть инструменты и навыки, чтобы содержать свой дом в порядке. Он отметил, что медиа-организации могут быть самыми разнообразными и часто имеют множество движущихся частей с конкурирующими приоритетами в отношении доступа и безопасности.

«Может быть много поддерживающих поставщиков с множеством точек соприкосновения для клиентов, создателей и широкой публики», — сказал он. «К сожалению, во многих из этих организаций группы кибербезопасности недоукомплектованы кадрами и ресурсами».

Молинофф сказал, что в отношении управления рисками поставщиков наиболее важными моментами являются выявление и классификация поставщиков на основе потенциального риска кибербезопасности, который они могут представлять для организации.

Кроме того, отрасль в целом должна постоянно отслеживать состояние кибербезопасности своих поставщиков, а также цифровое взаимодействие и/или обмен данными с ними.

Наконец, медиа-компании должны помочь своим поставщикам снизить критические риски, которые могут повлиять на них.

«Критические уязвимости часто эксплуатируются в течение нескольких минут после того, как общедоступный код проверки концепции становится общедоступным», — добавил он.

Бад Брумхед, генеральный директор Viakoo, поставщика средств автоматизированной гигиены кибербезопасности IoT, отметил, что медиа-организации являются сокровищницей ценных данных, а также могут выступать в качестве стартовой площадки для атак.

«Специализированное оборудование, используемое в медиапроизводстве, является формой Интернета вещей, и традиционные решения в области ИТ-безопасности не могут предотвратить или устранить кибератаки против них», — сказал он. «Это означает, что даже такие задачи, как обновление прошивки или смена паролей, требуют ручных усилий, если для автоматизации этих задач не используется специальная платформа безопасности IoT».

Он сказал, что системы управления контентом предлагают злоумышленникам платформу, предназначенную для совместного использования и распространения (т. е. переноса вредоносных полезных нагрузок), а также возможность доступа, манипулирования и изменения данных.

Брумхед добавил, что из-за высокой ценности медиа-контента и того, как он предназначен для совместного использования и распространения, злоумышленники всегда будут стремиться использовать уязвимости через медиа-организации и системы управления контентом.

«Ожидайте более широкого использования эксфильтрованных медиаданных для создания дипфейков и использования медиаконтента для нарушения биометрической безопасности», — предупредил он. «Поскольку медиа-организации используют высокопроизводительные вычисления, злоумышленники, скорее всего, широко используют эту вычислительную мощность для организации более масштабных и ресурсоемких атак». ***(Nathan Eddy. Cybersecurity Woes, Lax Patching Puts Media Companies At Risk // Techstrong Group Inc. (https://securityboulevard.com/2022/09/cybersecurity-woes-lax-patching-put-media-companies-at-risk/). 08.09.2022).***

***

«Apple выпустила обновления безопасности для устранения восьмой уязвимости нулевого дня, используемой в атаках на iPhone и Mac с начала года.

В бюллетенях по безопасности, опубликованных в понедельник, Apple сообщила, что им известны сообщения о том, что эта уязвимость «могла быть активно использована».

Ошибка (отслеживаемая как CVE-2022-32917) может позволить вредоносным приложениям выполнять произвольный код с привилегиями ядра.

Как сообщил Apple анонимный исследователь, проблема была устранена в iOS 15.7 и iPadOS 15.7, macOS Monterey 12.6 и macOS Big Sur 11.7 с улучшенными проверками границ.

Полный список затронутых устройств включает:

iPhone 6s и новее, iPad Pro (все модели), iPad Air 2 и новее, iPad 5-го поколения и новее, iPad mini 4 и новее, а также iPod touch (7-го поколения).

и компьютеры Mac под управлением macOS Big Sur 11.7 и macOS Monterey 12.6.

Apple также перенесла исправления для еще одного нулевого дня (CVE-2022-32894) на компьютеры Mac под управлением macOS Big Sur 11.7 после выпуска дополнительных обновлений безопасности 31 августа для устранения той же ошибки в версиях iOS, работающих на старых iPhone и iPad.

Хотя Apple сообщила об активном использовании этой уязвимости в дикой природе, компания еще не опубликовала никакой информации об этих атаках.

Отказываясь публиковать эту информацию, Apple, вероятно, хочет позволить как можно большему количеству клиентов исправлять свои устройства до того, как другие злоумышленники разработают свои собственные эксплойты и начнут использовать их в атаках, нацеленных на уязвимые iPhone и Mac.

Хотя этот нулевой день, скорее всего, использовался только в узконаправленных атаках, по-прежнему настоятельно рекомендуется устанавливать эти обновления безопасности как можно скорее, чтобы блокировать попытки атак…». ***(Sergiu Gatlan. Apple fixes eighth zero-day used to hack iPhones and Macs this year // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/apple-fixes-eighth-zero-day-used-to-hack-iphones-and-macs-this-year/). 12.09.2022).***

***

«CISA добавила две новые уязвимости в свой список ошибок безопасности, используемых сегодня в дикой природе, в том числе уязвимость повышения привилегий Windows и уязвимость выполнения произвольного кода, затрагивающую iPhone и Mac.

Ошибка повышения привилегий в общем системном драйвере файлов журнала Windows отслеживается как CVE-2022-37969, что позволяет локальным злоумышленникам получить системные привилегии после успешной эксплуатации.

Microsoft исправила уязвимость, обнаруженную и о которой сообщили исследователи из DBAPPPSecurity, Mandiant, CrowdStrike и Zscaler во время вторника исправлений в сентябре 2022 года.

«Мы обнаружили эту ошибку 0Day во время упреждающей миссии по поиску эксплойтов Offensive Task Force. Эксплойт повышения привилегий (EOP) был обнаружен в дикой природе, используя эту уязвимость Common Log File System (CLFS)», — Дханеш Кижаккинан, старший главный инженер по уязвимостям в Mandiant, сообщил BleepingComputer.

«Похоже, эксплойт является автономным, а не частью цепочки (например, браузер + EOP)».

Apple также исправила уязвимость выполнения произвольного кода (CVE-2022-32917) в понедельник и подтвердила, что она использовалась в атаках как ошибка нулевого дня в ядре iOS и macOS.

Это была восьмая уязвимость нулевого дня, используемая Apple с начала года, и все они, скорее всего, использовались только в узконаправленных атаках.

Федеральным агентствам приказано исправить в течение трех недель

Обязательная операционная директива (BOD 22-01), выпущенная в ноябре 2021 года, гласит, что все агентства Федеральной гражданской исполнительной власти (FCEB) должны защищать свои сети от ошибок, добавленных в каталог известных эксплуатируемых уязвимостей (KEV) CISA.

CISA предоставила агентствам Федеральной гражданской исполнительной власти (FCEB) три недели, до 10 октября, для устранения этих двух недостатков безопасности и блокирования атак, которые могут быть нацелены на их системы.

Несмотря на то, что директива применяется только к федеральным агентствам США, агентство по кибербезопасности настоятельно призвало все организации исправить эскалацию привилегий Windows и недостатки выполнения кода ядра Apple, чтобы предотвратить попытки эксплуатации.

«Эти типы уязвимостей являются частым вектором атак для злоумышленников и представляют значительный риск для федерального предприятия», — предупредил сегодня CISA.

С тех пор как BOD 22-01 был выпущен, CISA добавила более 800 недостатков безопасности в каталог ошибок, используемых в дикой природе, требуя, чтобы федеральные агентства устраняли их в более сжатые сроки, чтобы блокировать атаки и потенциальные нарушения безопасности». ***(Sergiu Gatlan. CISA orders agencies to patch Windows, iOS bugs used in attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/cisa-orders-agencies-to-patch-windows-ios-bugs-used-in-attacks/). 14.09.2022).***

***

«Кибератаки, направленные на уязвимости в интернет-браузерах, растут, и Google Chrome все чаще попадает в поле зрения хакеров.

Согласно анализу, проведенному исследователями кибербезопасности из WatchGuard, во втором квартале этого года количество вредоносных атак на браузеры — Chrome, Firefox и Internet Explorer — увеличилось на 23% по сравнению с предыдущим кварталом.

Большая часть этого роста была вызвана ростом кибератак на Chrome: согласно отчету WatchGuard Threat Lab Internet Security Report количество атак, нацеленных на браузер Google, увеличилось на 50%.

Браузеры представляют интерес для хакеров, потому что они играют ключевую роль в том, как мы пользуемся Интернетом — вводим и храним информацию, включая пароли, файлы cookie и даже данные кредитной карты. Это делает их мишенью для вредоносных программ, похищающих информацию.

Вся эта информация полезна киберпреступникам, чтобы они могли использовать себя или продавать на форумах даркнета для использования другими. Например, украденные пароли для корпоративных облачных сервисов могут быть использованы для запуска масштабных кибератак, включая кампании программ-вымогателей, а данные украденных карт могут использоваться для опустошения банковских счетов людей.

Исследователи предполагают, что одной из причин роста числа атак на Chrome может быть сохранение различных эксплойтов нулевого дня.

В этом году было несколько случаев таких серьезных уязвимостей Chrome, включая CVE-2022-1364, CVE-2022-2294 и CVE-2022-307. Google предупредил, что последний активно используется для проведения кибератак, а пользователям браузера Chrome на Windows, Mac и Linux было рекомендовано немедленно установить соответствующее обновление безопасности.

Однако исследователи предполагают, что рост числа атак на Chrome может быть частично связан с тем, что многие браузеры не получают обновления, особенно если администраторы не применяют автоматически исправления безопасности. Без этих обновлений браузеры очень уязвимы для атак.

Обеспечение скорейшего применения критических обновлений безопасности — одна из лучших стратегий, когда речь идет о защите от кибератак, направленных на браузеры или любое другое программное обеспечение.

«Все, что нужно, — это одна неисправленная уязвимость, чтобы атака протиснулась через брешь в вашей защите. Постоянное обновление вашего программного обеспечения с помощью последних исправлений безопасности — это одно из лучших действий, которое вы можете предпринять с точки зрения отдачи от вложенных средств в киберзащите», - говорится в отчете WatchGuard». ***(Danny Palmer. There's been a big rise in hackers targeting Google Chrome - doing this one thing can help protect you // ZDNET (https://www.zdnet.com/article/theres-been-a-big-rise-in-hackers-targeting-google-chrome-doing-this-one-thing-can-help-protect-you/). 28.09.2022).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Accenture (NYSE: ACN) была названа лидером в области услуг ИТ-безопасности в Северной Америке и Европе в двух новых отчетах аналитической компании Everest Group.

В обоих отчетах — «Оценка Everest IT Security Services PEAK Matrix® Assessment 2022 — Северная Америка» и «Everest IT Security Services PEAK Matrix® Assessment 2022 — Европа» — компания Accenture позиционируется как лидер и получает наивысшие баллы по обоим параметрам оценки: Vision & Возможность; и Влияние на рынок. В обоих отчетах отмечается, что клиенты ценят Accenture за ее способность выполнять комплексные обязательства по обеспечению безопасности, а также за ее глубокие и технические знания и считают ее стратегическим партнером в области безопасности.

Accenture заняла первое место среди всех 27 провайдеров, оцененных в отчете по Северной Америке, в котором отмечается:

Accenture внедрила автоматизацию своих служб безопасности, что привело к сокращению количества ложных предупреждений, более быстрому обнаружению угроз и более быстрому анализу журналов безопасности для клиентов.

Инвестиции компании в количественную оценку кибер-рисков для руководителей на уровне совета директоров, которая обеспечивает единое представление о рентабельности инвестиций в кибербезопасность для руководителей на уровне совета директоров.

Accenture использует технологии безопасности следующего поколения и глобальные ресурсы для улучшения операций по обеспечению безопасности и более эффективного прогнозирования атак, локализации нарушений, минимизации уязвимостей и обеспечения непрерывности бизнеса.

В европейском отчете Accenture опережает всех 28 поставщиков, оцененных Everest Group, подчеркивая:

Комплексные и отраслевые предложения безопасности Accenture охватывают весь образ жизни в области безопасности, от киберстратегии до киберустойчивости и киберзащиты.

Компания работает с клиентами, от опытных практиков до руководителей высшего звена, рассматривая безопасность как ускоритель бизнеса, обеспечивая инвестиции клиента в преобразующие решения и предоставляя достоверную ценность на 360 градусов, переосмысливая бизнес-киберзащиту, созданную для будущего.

Что корпоративные покупатели, которые ищут услуги по обеспечению соблюдения Общего регламента по защите данных (GDPR) и операционных технологий (OT), оценят ценные инструменты оценки зрелости Accenture, поскольку они обеспечивают широкий охват государственных норм и требований.

«Для нас большая честь быть признанным Everest Group лидером в сфере услуг по обеспечению ИТ-безопасности как в Северной Америке, так и в Европе, — сказал Паоло Даль Чин, глобальный руководитель Accenture Security. «Мы стремимся помочь обезопасить мир, и мы надеемся достичь этого, предоставив нашим клиентам инновационные услуги в области ИТ-безопасности. Мы продолжим уделять особое внимание защите от современных киберугроз, а также технологий, которые будут иметь решающее значение для бизнеса наших клиентов в будущем. Безопасность всегда находится на переднем крае нашей инновационной стратегии».

В обоих отчетах также отмечается, что предприятия, желающие инвестировать в безопасность следующего поколения, сочтут Accenture привлекательной благодаря ее обширным инвестициям в инновации и решения нового поколения, такие как удостоверения личности на основе блокчейна, безопасность подключенных автомобилей и решение для безопасности цифровых двойников — CyTwin.

Кумар Авиджит, директор по практике Everest Group, сказал: «Ключом к успешному предоставлению услуг ИТ-безопасности является создание контекстуализированных дорожных карт для клиентов, а не измерение всего одним и тем же критерием. Акцент Accenture на конвергентной безопасности ИТ/OT и опыт в области кибербезопасности нового века, а также развитие собственных кадров позволяют ей предоставлять индивидуальные инновационные услуги в области ИТ-безопасности. Клиенты высоко оценили способность Accenture позиционировать себя как стратегического партнера с сильными техническими и отраслевыми возможностями, продемонстрированными ее талантом в области ИТ-услуг по кибербезопасности. Эти факторы способствовали тому, что компания Everest Group

заняла лидирующие позиции в рейтинге услуг ИТ-безопасности PEAK Matrix® Assessment 2022 — Северная Америка и Европа».

Everest Group отмечает в обоих отчетах, что предприятия выиграют от комплексного набора решений Accenture, который охватывает такие темы безопасности, как безопасность OT, безопасность приложений, облачная безопасность, управление идентификацией и доступом, а также нулевое доверие. В Соединенных Штатах компания Accenture недавно присоединилась к Объединенной группе по киберзащите (JCDC) Агентства по кибербезопасности и безопасности инфраструктуры (CISA), в состав которой теперь входят эксперты по промышленным системам управления (ICS).

Помимо того, что Accenture была названа лидером в области услуг ИТ-безопасности в Северной Америке и Европе, компания Accenture была названа лидером и лидером в отчете Everest PEAK Matrix® для услуг ИТ-безопасности за 2020 год…» ***(Accenture Scored the Highest in IT Security Services in North America and Europe by Everest Group // NATIONAL CYBER SECURITY NEWS TODAY (https://nationalcybersecuritynews.today/accenture-scored-the-highest-in-it-security-services-in-north-america-and-europe-by-everest-group-cloudsecurity/). 21.09.2022).***

***

«Компании должны быть уверены, что их инфраструктура защищена от цифровых угроз. Низкая безопасность данных может привести к утечке данных и инцидентам безопасности, которые негативно скажутся на бизнесе и его клиентах.

Если кибератаки не обнаруживаются и не устраняются своевременно, последствия могут быть дорогостоящими, трудоемкими и приводить к потере конфиденциальной информации.

Со временем киберпреступники усовершенствовали свои методы обхода базовых решений безопасности. Поэтому предприятиям требуется надежный план обеспечения безопасности.

Использование расширенных платформ обнаружения и реагирования (XDR) может повысить уровень безопасности организации.

XDR — это платформа, которая обеспечивает прозрачность, возможности обнаружения и эффективное реагирование на угрозы в корпоративной среде.

Представляем Вазу

Wazuh — это бесплатная платформа безопасности с открытым исходным кодом, которая обеспечивает унифицированную защиту SIEM и XDR. Он защищает рабочие нагрузки в локальных, виртуализированных, контейнерных и облачных средах.

Платформа Wazuh использует модель сервера/агента:

Центральные компоненты Wazuh (сервер, индексатор и информационная панель), которые анализируют данные безопасности, собранные с агентов. Их можно настроить локально или в облаке с помощью решения Wazuh Cloud.

Облегченные и универсальные агенты безопасности развертываются на контролируемых конечных точках для сбора данных о безопасности и автоматического реагирования на угрозы.

Решение Wazuh также обеспечивает безагентный мониторинг таких устройств, как маршрутизаторы, брандмауэры и коммутаторы, которые не поддерживают установку агентов…

Безопасность конечной точки

Wazuh предоставляет возможности для предотвращения, обнаружения и реагирования на угрозы. Агенты Wazuh, установленные на конечных точках, выполняют следующие действия:

Соберите данные безопасности.

Сообщайте о неправильных конфигурациях и проблемах безопасности.

Отслеживайте файловую систему и сообщайте об изменениях.

Помимо наблюдения за безопасностью и мониторинга конечных точек, Wazuh предоставляет возможности самозащиты и автоматических ответов на обнаруженные угрозы. Решение Wazuh может выполнять реагирующие действия, такие как удаление вредоносных файлов, блокирование вредоносных сетевых подключений и другие меры противодействия.

Операции безопасности

Важной особенностью XDR является его способность агрегировать, нормализовать и сопоставлять данные из нескольких источников. Wazuh собирает большие объемы событий на различных устройствах и анализирует их для получения ценной информации о безопасности.

Агенты безопасности имеют модуль обнаружения аномалий и вредоносных программ, который обнаруживает аномальные и вредоносные события на конечных точках.

Wazuh поддерживает соответствие нормативным требованиям, используя наборы правил, которые тщательно сопоставлены с требованиями соответствия. Wazuh обеспечивает готовую поддержку таких систем соответствия, как PCI DSS, HIPAA, GDPR, NIST SP 800-53 и TSC.

Аналитика угроз

Исследователи кибербезопасности и злоумышленники продолжают находить и использовать уязвимости в компьютерных системах. Поэтому для предприятий важно знать о старых и новых уязвимостях, присутствующих в их ИТ-инфраструктуре.

Wazuh имеет встроенный модуль обнаружения уязвимостей, который периодически сканирует установленные приложения на наличие уязвимостей. Он сопоставляет данные, полученные от конечных точек, с актуальными базами данных CVE (Common Vulnerabilities and Exposure) и обеспечивает видимость безопасности.

Решение Wazuh также включает платформу MITRE ATT&CK для быстрого распознавания и поиска тактик, методов и процедур (TTP) злоумышленников в корпоративной среде. Оповещения о событиях сопоставляются со связанными с ними методами MITRE ATT&CK, чтобы включать полезную информацию.

Облачная безопасность

Предприятия все чаще полагаются на облачные решения для размещения своих услуг. В этом отношении Wazuh обеспечивает защиту в режиме реального времени не только для локальных рабочих нагрузок, но и для облачной инфраструктуры.

Его можно интегрировать с облачными сервисами, такими как Google Cloud Platform (GCP), Amazon Web Services (AWS) и Microsoft Azure, для обеспечения безопасности этих инфраструктур на уровне облака. Делая еще один шаг вперед, решение Wazuh учитывает контейнерные рабочие нагрузки, обеспечивая защиту популярных технологий, таких как Docker и Kubernetes.

Бесплатный и с открытым исходным кодом

Wazuh — одно из самых быстрорастущих решений для обеспечения безопасности с открытым исходным кодом, которое загружают более 10 миллионов раз в год. Wazuh предоставляет сообщества, в которых пользователи могут взаимодействовать с разработчиками Wazuh, делиться опытом и задавать вопросы, связанные с платформой.

Бесплатный и открытый исходный код предоставляет возможность масштабирования и настройки. Эту платформу можно легко интегрировать с другими инструментами и решениями безопасности с открытым исходным кодом для расширения возможностей XDR. Некоторые из его интеграций включают VirusTotal, Suricata, YARA и Slack, и это лишь некоторые из них. Ознакомьтесь с этой документацией о том, как начать работу с Wazuh». ***(Wazuh - The free and open source XDR platform // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/wazuh-the-free-and-open-source-xdr-platform/). 28.09.2022).***

***