Науково-дослідний інститут інформатики і права
Національної академії правових наук України
Національна бібліотека України імені В. І. Вернадського

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 1 (січень)

Київ – 2021

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К., 2021.– №1 (січень) . – 297с.

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.

© Науково-дослідний інститут інформатики і права Національної академії правових наук України, 2021

© Національна бібліотека України імені В.І. Вернадського, 2021

ЗМІСТ

Стан кібербезпеки в Україні 4
Правове забезпечення кібербезпеки в Україні 9
Кібервійна проти України 9
Боротьба з кіберзлочинністю в Україні 11
Коронавірус COVID-19 та питання кібербезпеки 18
Світові тенденції в галузі кібербезпеки 24
Сполучені Штати Америки 43
Країни ЄС та Великобританія 73
Російська Федерація та країни ЄАЕС 76
Інші країни 79
Протидія зовнішній кібернетичній агресії 79
Створення та функціонування кібервійськ 86
Кібератака на SolarWinds 88
Кіберзахист критичної інфраструктури 109
Захист персональних даних 111
Кібербезпека Інтернету речей 167
Кіберзлочинність та кібертерроризм 175
Діяльність хакерів та хакерські угруповування 203
Вірусне та інше шкідливе програмне забезпечення 207
Операції правоохоронних органів та судові справи проти кіберзлочинців 253
Технічні аспекти кібербезпеки 259
Виявлені вразливості технічних засобів та програмного забезпечення 267
Технічні та програмні рішення для протидії кібернетичним загрозам 292

«В 2020 году Украина впервые была представлена в Европейском рейтинге открытости данных – 17 место из 35 в числе стран, которые быстро развиваются. Украина набрала 2 180 баллов из 2 600 возможных: государственная политика (соответствие законодательства международным стандартам, стратегия по развитию сферы открытых данных) – 554 балла, Единый государственный веб-портал открытых данных – 569 баллов, влияние открытых данных в различных сферах (экономической, социальной, экологической и так далее) – 550 баллов, качество опубликованных на портале данных – 492 балла.

Первое место в рейтинге открытости данных в 2020 году заняла Дания, последнее – Лихтенштейн.

Не так давно, с 2018 года, Украина фигурирует в рейтинге кибербезопасности. Его составитель – эстонская Академия электронного управления – анализирует законодательство стран в сфере кибербезопасности, обеспечение защиты услуг, защиту персональных данных, меры по реагированию на кибератаки, борьбу с киберпреступностью.

В 2018 году Украина занимала в рейтинге 29 место из 160, в 2020 году – 25-е. Первенство отдали Греции, последний в списке – Южный Судан.

Украина опустилась в рейтинге счастья: 2015 год – 111 место, 2016-й – 123 место, 2017-й – 132 место, 2018-й – 138 место, 2019-й – 133 место. В прошлом году нам удалось немного вернуть позиции – 123 место из 152. Самыми счастливыми оказались жители Финляндии, самыми несчастными – жители Афганистана. Напомним, при составлении рейтинга учитывается уровень ВВП страны, ожидаемая продолжительность жизни, уровень коррупции, занятость, уровень доверия в обществе, наличие гражданских свобод.

В 2020 году Украина поднялась в мировом рейтинге владения английским языком – на 44 место из 100 (это средний уровень). В первую тройку лидеров вошли Нидерланды, Дания и Финляндия, в тройку аутсайдеров – Оман, Ирак и Таджикистан.

В 2015 году наша страна занимала 34 место, в 2016-м – 41-е, в 2017-м – 47 место, в 2018-м – 43-е, в 2019-м – 49 место.

Есть прогресс в глобальном рейтинге инноваций. В 2015 году Украина занимала 64 место, в 2016-м – 56 место, в 2017-м – 50 место, в 2018-м – 43 место, в 2019-м – 47 место. В 2020 году Украина поднялась на 45 место из 131. Лидирует Швейцария, последний в списке – Йемен.

В рейтинге экономической свободы Украина сильно откатилась назад в 2017 году: если в 2015-м наше государство было на 128 месте, то в 2017-м – на 149-м. При оценивании стран учитываются 44 показателя из 5 сфер экономической свободы: монетарная политика, отсутствие ограничений в международной торговле, размер правительства и так далее.

В 2020-м Украина улучшила свою позицию, заняв 131 место. На первом оказался Гонконг, на последнем – Венесуэла». ***(Как менялось место Украины в мировых рейтингах в 2015-2020 годах // Слово и дело***

(https://ru.slovoidilo.ua/2021/01/05/infografika/obshhestvo/kak-menyalos-mesto-ukrainy-mirovyx-rejtingax-2015-2020-godax). 05.01.2021).

***

«В декабре команда Министерства цифровой трансформации при поддержке агентства по международному развитию США (USAID) провела на платформе Bugcrowd тестирование сервиса Дия. Уязвимостей, которые бы влияли на безопасность не было найдено. Хакеры смогли обнаружить только два технических бага низкого уровня, которые сразу были исправлены разработчиками Дия, говорится на сайте Минцифры.

Среди найденных во время багбаунти багов ведомство отмечает следующие пункты:

Возможность сгенерировать такой QR-код, при считывании которого мобильное приложение вылетает с ошибкой. Эта проблема не влияет на безопасность данных пользователей, поэтому получила самый низкий приоритет уровня P5.

Возможность получения информации о полисе страхования автомобиля пользователя при модификации приложения, если известен госномер авто и VIN-код. Поскольку эта информация и так есть в открытом доступе и не содержит данных пользователя или сервиса, которые бы подпадали под защиту Закона "О защите персональных данных", такая уязвимость получила уровень P4.

Представители платформы Bugcrowd сообщили, что специалисты, выявившие уязвимость уровня P4 получат $250 из общего призового фонда, который составил $35 000. Обнаружение бага уровня P5 по условиям программы не предусматривало выплат из призового фонда.

Баг-баунти (Bug Bounty) – это процесс, в котором компания привлекает сторонних специалистов по кибербезопасности для тестирования своего программного обеспечения на уязвимости. За каждую найденную уязвимость (баг) люди получают вознаграждение (баунти). Всего, к баг-баунти приложения Дія были привлечены 84 специалистов, которые соответствуют заданным критериям, 14 из которых – украинцы». ***(Ирина Скиба. $250 вместо миллиона. Поиск уязвимостей в Дие закончился провалом для белых хакеров // AOinform (https://www.aoinform.com/news/250_vmesto_milliona_poisk_ujazvimostej_v_die_zakonchilsja_provalom_dlja_belykh_khakerov/2021-01-01-42117). 01.01.2021).***

***

«Министерство внутренних дел Украины совместно с Киберполицией создали современный классификатор онлайн-угроз. Об этом сообщила заместитель Министра внутренних дел Татьяна Ковальчук в ходе конференции по вопросам безопасности человека в онлайн-пространстве «Международная конференция «Безопасный онлайн 2020: Современные вызовы», передает kurs.com.ua.

Опыт создания подобного классификатора есть только в нескольких ведущих странах мира, в частности в Великобритании, отметили в МВД. К созданию

классификатора были привлечены лучшие наработанные мировым сообществом практики, с более расширенным и структурированным видом, который будет максимально отвечать украинским реалиям и контенту.

Классификатор онлайн-угроз включает следующие киберугрозы:

- Дезинформация и манипуляция.
- Нарушение авторских прав.
- Пропаганда насилия, террористической и экстремистской деятельности.
- Распространение через Интернет запрещенных и ограниченных к продаже товаров и услуг.
- Мошенничество в онлайн-пространстве.
- Доступ детей к вредоносному контенту.
- Жестокое обращение с детьми в сети Интернет, сексуальная эксплуатация и развращение детей в киберпространстве.
- Чрезмерное использование экранного времени.
- Киберпреследование и кибертравля.
- Пропаганда суицида и самокалечения.

«Мы выводим наше государство в лигу мировых лидеров по работе с информационной безопасностью», - подытожила Татьяна Ковальчук». ***(В Украине разработан классификатор онлайн-угроз // Судово-юридична газета (https://sud.ua/ru/news/ukraine/190891-v-ukraine-razrabotan-klassifikator-onlayn-ugroz). 20.01.2021).***

***

«Міністерство цифрової трансформації та координатор проєктів ОБСЄ в Україні запустили освітній серіал для держслужбовців «Основи кібергігієни». Як повідомляє пресслужба Мінцифри, серіал складається з 9 серій тривалістю 4-7 хвилин.

«Серіал рекомендується державним службовцям та посадовим особам органів місцевого самоврядування. Після перегляду всіх серій та складання фінального тестування кожен отримає сертифікат, що засвідчує успішне проходження базового курсу з цифрової грамотності обсягом», - говориться у повідомленні.

Участь у створенні серіалу взяли:

Ілона Довгань, теле- та радіоведуча, медіаекспертка Координатора проєктів ОБСЄ в Україні

Демид Майорников, національний експерт з кібербезпеки Координатора проєктів ОБСЄ в Україні

Ольга Войтович, національна спеціалістка проектів Координатора проєктів ОБСЄ в Україні

Серіал доступний у безкоштовному доступі на онлайн-платформі Дія.Цифрова освіта…». ***(Мінцифри створило серіал про кібергігієну для чиновників // MediaSapiens (https://ms.detector.media/trendi/post/26493/2021-01-27-mintsyfry-stvorylo-serial-pro-kibergigiienu-dlya-chynovnykiv/). 27.01.2021).***

***

«Національний банк України впровадить виїзні перевірки та безвиїзний нагляд щодо дотримання банками заходів кіберзахисту та інформаційної безпеки

Про це повідомила пресслужба НБУ.

Згідно з повідомленням, НБУ посилює контроль за виконанням банками заходів із забезпечення кіберзахисту та інформаційної безпеки. Для цього регулятор запроваджує новий вид контролю за банками у формі виїзних перевірок та безвиїзного нагляду. Заходи здійснюватимуться фахівцями НБУ у сфері кіберзахисту та інформаційної безпеки.

Крім того, банки будуть зобов'язані проводить щорічну самооцінку стану інформаційної безпеки та кіберзахисту, а також складати і подавати НБУ щорічний звіт з питань оцінювання відповідних ризиків.

Зазначається, що реалізація таких механізмів контролю дозволить НБУ оцінювати ефективність функціонування системи управління інформаційною безпекою банку, повноту виконання банком нормативно-правових актів з питань інформаційної безпеки та кіберзахисту, а також рівень управління банку ризиками інформаційної безпеки й кіберризиків, системи внутрішнього контролю за цими напрямками». ***(НБУ почне перевірки банків на дотримання кібербезпеки // Espreso.tv (https://espreso.tv/news/2021/01/21/nbu_pochne_perevirky_bankiv_na_dotrymannya_kiberbezpeky). 21.01.2021).***

***

«Україна взяла курс на інтеграцію в європейський цифровий простір.

Імплементація положень Угоди про асоціацію (в тому числі оновленого Додатка XVII-3) дозволить Україні поступово наблизитися до цифрового ринку ЄС.

Це призведе до зменшення бар’єрів та обмежень у торгівлі з ЄС та прискорення розвитку цифрової економіки в Україні.

Наразі Україна відстає від країн-членів ЄС та навіть країн-сусідів за рівнем цифрового розвитку.

Про це свідчать дані міжнародних рейтингів, таких як EGDI, NRI, WDCR. Аби скоротити відставання (принаймні з країнами-сусідами) необхідно прискорити цифрову трансформацію, зокрема у найслабших сферах: регуляторному середовищі, розвитку телекомунікаційної інфраструктури і впровадженні державою цифрових технологій. Такі зміни необхідні для інтеграції або хоча б наближення України до єдиного цифрового ринку (ЄЦР) ЄС.

І це – не порожні слова. За оцінкою експертів Центру досліджень міжнародної торгівлі Trade+ Київської школи економіки, збільшення цифровізації української економіки та суспільства на 1% може призвести до зростання ВВП України на 0,42%.

Відповідно, залежно від рівня цифровізації, до якого поступово наближатиметься Україна в рамках ЄЦР ЄС, позитивний кумулятивний вплив на ВВП України може скласти від 2,4 до 12,1% ($3,1-15,8 млрд) додаткового зростання протягом усього періоду наближення…

Крім того, Україна виграє від скорочення торговельних витрат у двосторонній торгівлі з ЄС внаслідок зменшення регуляторних цифрових бар’єрів, що позитивно вплине на добробут громадян (потенційне покращення на 3,6-7,8%).

Усунення бар'єрів для транскордонної цифрової торгівлі підвищує загальну ефективність ЗВТ з ЄС.

ЄЦР спрощує та зменшує вартість транскордонних електронних транзакцій, покращує транскордонний доступ до онлайн-ринків та інноваційних цифрових продуктів і послуг для бізнесу та споживачів.

Цифровізація торгівлі за європейськими правилами активізує загальну торгівлю товарами та послугами з ЄС – спрощує експортні процедури, зменшує торговельні витрати експортерів, створює нові можливості для торгівлі з ЄС, зокрема це стосується малого та середнього бізнесу.

Як наслідок, до переваг єдиного ринку з Євросоюзом належать зниження цін, більший вибір товарів та послуг та покращення зручності для споживачів і бізнесу, ефект економії від масштабу для українського бізнесу завдяки кращому доступу на великий європейський ринок, посилення захисту прав споживачів онлайн послуг.

Проте, аби всі ці плани й розрахунки втілились у реальність, Україні необхідно виконати чергове "домашнє завдання".

Компонентами єдиного цифрового ринку ЄС, які потребують удосконалення в Україні, є:

електронна ідентифікація,

платіжні системи, електронні платежі та розрахунки,

захист прав інтелектуальної власності в інтернеті,

кібербезпека та захист персональних даних.

Крім того, регуляторне середовище України є досить обмежувальним щодо цифрової торгівлі. Тут найбільше бар’єрів пов’язано з:

- транскордонними електронними платежами та транскордонними електронними транзакціями (відсутністю механізмів для застосування електронного цифрового підпису в зовнішньоекономічних контрактах, відсутністю взаємного визнання електронної ідентифікації та електронних довірчих послуг між Україною та основними торговельними партнерами тощо),

- технічними вимогами щодо використання місцевого програмного забезпечення та криптографії.

Подолання цих бар’єрів необхідне для інтеграції України у європейський та глобальний цифровий простір, який все більше впливає на міжнародну торгівлю і глобальну економіку.

Тож Україні варто поквапитися, бо з кожним днем ціна нашого відставання стає все більшою». ***(Світлана Таран, Любов Акуленко. Що дасть Україні інтеграція у цифровий простір ЄС // Європейська правда (https://www.eurointegration.com.ua/experts/2021/01/25/7118582/). 25.01.2021).***

***

«Верховна Рада ухвалила в першому читанні законопроєкт про реформу Служби безпеки України…

За проєкт закону № 3196-д проголосували 285 народних депутатів.

Законопроєкт спрямований "на підвищення інституційної спроможності Служби безпеки України щодо забезпечення державної безпеки й приведення законодавства, що регулює її діяльність, у відповідність із сучасними викликами та загрозами".

Законопроєкт має замінити закони "Про Службу безпеки України" та "Про загальну структуру і чисельність Служби безпеки України", якими зараз регулюється діяльність СБУ.

Проєкт закону надає можливість звільнити СБУ від невластивих для неї функцій. Так, серед іншого, ліквідуються спецпідрозділи СБУ з боротьби з корупцією та організованою злочинністю.

Відтак, Служба безпеки не займатиметься невластивими їй розслідуваннями економічних і корупційних злочинів.

Основними напрямами СБУ будуть контррозвідувальна діяльність, боротьба з тероризмом, захист національної державності, кібербезпека та охорона державної таємниці.

Пропонується розмежувати контррозвідувальний і оперативно-розшуковий види діяльності СБУ.

Планується істотно посилити напрям контррозвідувального захисту гілок влади.

Також особливу увагу в законопроєкті приділено: контррозвідувальному захисту економіки; недопущенню контролю над критичною інфраструктурою України з боку компаній, афілійованих до країни-агресора; попередженню підривної діяльності іноземних спецслужб в українському інформаційному просторі.

Істотно обмежується правоохоронна функція СБУ шляхом поступової, до 2024 року, передачі функції досудового розслідування в Державне бюро розслідувань.

Документом передбачена часткова демілітаризація Служби безпеки з переходом на спеціальні звання». ***(Рада підтримала за основу законопроєкт про реформу СБУ: що він передбачає // Букви (https://bykvu.com/ua/bukvy/rada-pidtrimala-za-osnovu-zakonoproiekt-pro-reformu-sbu-shho-vin-peredbachaie/). 28.01.2021).***

***

Кібервійна проти України

«Система захищеного доступу державних органів до мережі Інтернет заблокувала 76 328 атак різних видів, що на 32% більше, ніж попереднього

тижня. Переважна більшість - це мережеві атаки прикладного рівня (99%). Також зафіксовано і заблоковано 16 DDoS-атак, зокрема на вебресурси НАБУ та Держспецзв'язку".

Деталі: Система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури на об'єктах моніторингу зафіксувала 5 055 047 підозрілих подій, що на 17% більше, ніж попереднього тижня.

Переважна більшість зафіксованих підозрілих подій стосується спроб викрадення інформації (38%), мережевого сканування (27%), спроб отримання прав користувача (13%) та спроб отримання прав адміністратора (12%).

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 3 133 кіберінциденти, що на 5% більше, ніж попереднього тижня.

Переважна більшість опрацьованих інцидентів стосується недержавного сектору (близько 99%). Основна кількість інцидентів стосується розповсюдження шкідливого програмного забезпечення (99%).

Держспецзв'язку звертається до всіх: в разі будь-яких кіберінцидентів, кібератак або підозрілих дій щодо інформаційно-телекомунікаційних систем інформувати урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA». ***(В Україні зростає кількість кібератак // iPress (https://ipress.ua/news/v_ukraini_zrostaie_kilkist_kiberatak_317765.html). 06.01.2021).***

***

«Мошенники используют Facebook и Telegram, чтобы украсть страницы пользователя с целью наживы.

Они делают рассылку вредоносных сообщений, воруют аккаунты и с их помощью пишут друзьям жертвы сообщения, в которых от ее же имени просят одолжить денег, пишет "Обозреватель".

Эксперт в сфере кибербезопасности Глеб Пахаренко рассказал, что в последнее время случаи кибератак участились и возросло количество пострадавших. И, если раньше, злоумышленники вели охоту на крупные компании, то сейчас они не выбирают.

Они взламывают аккаунты для того, чтобы вымогать деньги на возврат доступа, делают рассылку от имени жертвы ее друзьям с просьбой одолжить денег, шантажируют личной информацией, которую получают из соцсетей и взломанных девайсов, а также получают доступ через программное обеспечение к мобильному банкингу.

Иногда восстановить аккаунт после таких вот взломов достаточно сложно - особенно, если мошенники сменили номер телефона.

"Если открыли линк от "друга", аккаунт которого взломали, можете попасть на рекламу, на папку загрузки. На устройство может быть загружена программа, которая после автоматически без подтверждения "доскачивает" другое вредоносное программное обеспечение. Иногда по линку можно попасть на сайт, который потребует ввести личные данные, данные банковской карты", – говорит

руководитель отдела внешних коммуникаций и маркетинга антивирусной компании Zillya! Владислав Андрианов.

Эксперты предупреждают об опасности установки на свои гаджеты подозрительных приложений, которые необходимы якобы для апгрейта приложений.

Скачивать необходимо только лицензированные приложения, а также нужна лицензированная версия операционной системы, обновленный браузер. Не открывать линки на неизвестные ресурсы - чаще всего мошенники присылают сокращенные ссылки которые начинаются с "bit.ly".» ***(Лидия Лыско. Используют социальные сети: украинцев массово начали разводить на деньги. Будьте внимательны // Hyser (https://light.hyser.com.ua/161332-ispolzuyut-socialnye-seti-ukraincev-massovo-nachali-razvodit-na-dengi-budte-vnimatelny).*** 10.01.2021).

***

Боротьба з кіберзлочинністю в Україні

«Ужгородский горрайонный суд Закарпатской области признал мужчину виновным во взломе аккаунтов украинцев в соцсетях и в создании и распространении вредоносных программ…

В феврале 2020 года злоумышленник создал канал в мессенджере «Telegram», на котором сначала писал статьи о различных аспектах информационной безопасности, а дальше начал предоставлять услуги "хакера".

Так, в марте 2020 года, через мессенджер «Telegram» он получил заказ от неустановленного досудебным расследованием лица на взлом аккаунта в социальной сети «Instagram». На что подсудимый согласился и назвал сумму 400 гривен и предоставил данные банковской карточки Приватбанка для получения денежных средств, на которую, после выполнения "работы", была зачислена вышеуказанная сумма.

Кроме этого, в апреле 2020 года, злоумышленник создал вредоносную программу для удаленного управления компьютером и распространил это ПО через мессенджер «Telegram» неустановленному количеству лиц.

Также, по данным следствия, в июне 2020 года обвиняемый загрузил ранее созданную вредоносную программу для скрытого майнинга на файлообменник в сети Интернет. Далее он создал тему на специальном форуме, в которой под видом другого программного обеспечения предоставил ссылки на загрузку данного файла.

Согласно заключению эксперта вышеуказанные файлы являются вредоносным программным средством.

1 декабря 2020 года между прокурором и обвиняемым было заключено соглашение о признании виновности, согласно которому подсудимый свою вину в совершении уголовных преступлений, предусмотренных ч.1 ст.361 и ч.1, 2 ст.361-1 УК Украины признал полностью и раскаивается в содеянном.

Учитывая вышеизложенное суд назначил мужчине наказание в виде лишения свободы сроком на 2 года с испытательным сроком в 1 год.

Также подсудимый должен оплатить в пользу государства расходы на проведение экспертизы в сумме 3217 грн. 47 коп». ***(Артем Сереженок. Хакер взламывал аккаунты украинцев в соцсетях и распространял вредоносные программы // Internetua (https://internetua.com/haker-vzlamyval-akkaunty-ukraincev-v-socsetyah-i-rasprostranyal-vredonosnye-programmy). 06.01.2021).***

***

«Суд приговорил к трем годам тюрьмы украинца, который взламывал учетные записи пользователей и продавал похищенную информацию в интернете…

Во время следствия было установлено, что злоумышленник с помощью собственного компьютерного оборудования, путем использования специализированного вредоносного программного обеспечения «Private Keeper», функционал которого позволяет подбирать логины и пароли по типу «брутфорс» (метод взлома, путем поочередного перебора возможных комбинаций) осуществлял несанкционированное вмешательство в работу автоматизированной системы интернет ресурса epicgames.com. Данный взлом привел к утечке информации учетных записей указанного сайта с возможностью отображения персональных данных и баланса учетных записей пользователей, что в соответствии со ст. 31 Конституции Украины и ч. 2 ст. 21 Закона Украины «Об информации», является информацией с ограниченным доступом.

6 июля 2020 года обвиняемый, используя свою учетную запись на одном из сайтов в Сети, за денежные средства в сумме 1500 грн., совершил несанкционированный сбыт информации с ограниченным доступом, а именно данные 10 учетных записей пользователей интернет-ресурсов с имеющимися действующими логинами в виде адресов электронной почты и паролями.

Таким образом, мужчину обвинили в совершении уголовных правонарушений, предусмотренных ч. 1 ст. 361 УК Украины (несанкционированное вмешательство в работу автоматизированных систем, что привело к утечке информации) и ч. 1 ст. 361-2 УК Украины (несанкционированый сбыт информации с ограниченным доступом, которая хранится в автоматизированных системах.

После завершения досудебного следствия обвиняемый и прокурор Черновицкой прокуратуры заключили соглашение о признании виновности на тех условиях, что мужчина полностью признает свою виновность в указанном выше преступлении, стороны соглашаются на назначение подсудимому наказания в виде лишения свободы сроком на три года с конфискацией программных и технических средств, с помощью которых было совершено несанкционированное вмешательство.

Суд утвердил данное соглашение. На основании ст.75 УК Украины суд своим решением освободил мужчину от отбывания наказания, если он в течение двух лет испытательного срока не совершит нового преступления и выполнит возложенные на него обязанности.

Также мужчина должен оплатить расходы за проведение судебных экспертиз в сумме 3922 грн. 80 коп». ***(Артем Сереженок. Хакер взламывал учетные записи***

украинцев и продавал похищенную информацию в интернете // Internetua (https://internetua.com/haker-vzlamyval-ucsetnye-zapisi-ukraincev-i-prodaval-pohisxennuua-informaciua-v-internete). 12.01.2021).

***

«Молодикові оголошено підозру у несанкціонованому збуті або розповсюдженні інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації. Йому загрожує до двох років позбавлення волі.

Співробітники кіберполіції Одещини спільно зі слідчими відділу поліції № 2 Одеського районного управління № 1 встановили, що місцевий житель за допомогою шкідливого програмного забезпечення, оминаючи антивірусні програми, викрадав логіни та паролі від поштових скриньок різних поштових ресурсів. Також одесит створив та адміністрував хакерський ресурс для розповсюдження викраденої конфіденційної інформації та надавав можливість іншим особам публікувати оголошення з продажу шкідливого програмного забезпечення і баз даних із конфіденційною інформацією.

За місцем проживання фігуранта правоохоронці провели обшук і вилучили комп’ютерну техніку, що використовувалася у протиправній діяльності.

Молодикові вже повідомлено про підозру за ч. 1 ст. 361-2 Кримінального кодексу України, санкція якої передбачає штраф від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або позбавлення волі на строк до двох років. Слідчі дії тривають.

Процесуальне керівництво здійснює Одеська місцева прокуратура №3». ***(В Одесі поліцейські припинили діяльність 21-річного хакера // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/v-odesi-policzejski-prypynyly-diyalnist--richnogo-xakera-1390/). 15.01.2021).***

***

«Фігурант у мережі перепродавав незаконно здобуті бази логінів і паролів користувачів різних соцмереж. За такі дії йому може загрожувати до двох років ув’язнення.

Правопорушення викрили співробітники відділу протидії кіберзлочинам Тернопільщини спільно зі слідчими місцевого відділу поліції.

Встановлено, що до протиправної діяльності причетний 28-річний житель Тернополя. Чоловік у Darknet купував бази із логінами та паролями користувачів різних соцмереж, які були здобуті завдяки використанню шкідливого програмного забезпечення. Далі правопорушник перевіряв їх на справність та здійснював їхню подальшу реалізацію.

За місцем мешкання фігуранта працівники поліції провели обшук та вилучили комп’ютерну техніку, яку буде направлено на експертизу.

Наразі кіберполіцейські встановлюють потерпілих від протиправної діяльності.

Відкрито кримінальне провадження за ч. 1 ст. 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в комп'ютерах, автоматизованих системах, комп'ютерних мережах) Кримінального кодексу України. Правопорушнику може загрожувати до двох років позбавлення волі. Слідчі дії тривають…» ***(Кіберполіція Тернопільщини викрила місцевого жителя у збуті конфіденційної інформації користувачів Інтернету // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-ternopilshhyny-vykryla-misczevogo-zhytelya-u-zbuti-konfidenczijnoyi-informacziyi-korystuvachiv-internetu-3836/). 13.01.2021).***

***

«Компьютерный "гений" из Закарпатья, который скромно работал оператором путеизмерительной тележки на железной дороге, решил найти «лучшее» применение своим интеллектуальным способностям и завел Telegram-канал, на котором стал публиковать статьи, посвященные различным аспектам компьютерной безопасности.

Когда канал набрал более 21 тысячи подписчиков, а его автор «прокачал» свою репутацию эксперта, он решил, что это можно как-то монетизировать и начал предлагать читателям услуги хакера.

Первый заказ, который он получил – была задача «увести» чужой Instagram-аккаунт. Для этой цели молодой человек создал интернет-страничку, внешне идентичную странице входа в социальную сеть Instagram, которая пересылала злоумышленникам все вводимые авторизационные данные. Ссылку на эту страницу он передал заказчику, который перечислил за работу 400 гривен на карточку Приватбанка.

Вторым заказом, который получил хакер – было разработать кейлоггер – программу-вирус, которая считывает нажатые на зараженном компьютере клавиши и помогает таким образом злоумышленникам получить в свое распоряжение нужную информацию, например, пароли. За выполнение этого заказа хакер заработал 600 гривен, которые также получил на карту Приватбанка.

Осознав, что много таким путем он не заработает, молодой человек придумал, как его знания и навыки могут обеспечить ему стабильный пассивный доход. Решение, которое пришло ему на ум – криптовалюта.

Как известно, криптовалюты сейчас очень популярны. При этом, стоимость самой популярной из них – Bitcoin - постоянно растет. «Добываются» биткойны путем «майнинга» - произведения вычислений компьютерной техникой. Около 10 лет назад такие вычисления еще можно было производить обычным компьютером, но, со временем, они становились все сложнее, так что майнерам приходилось приобретать все более сложное оборудование – высокопроизводительные видеокарты.

Еще один возможный путь майнинга – это создание целого кластера объединенных сетью компьютеров, которые производят вычисления, в результате которых появляются новые токены (монеты). Именно это и решил реализовать

молодой человек - заставить чужие компьютеры генерировать для него электронные деньги.

В качестве проверки своих сил, он разработал вирус, который перехватывал управление зараженным компьютером и производил некоторые заметные пользователю действия. Назвав его «лол.exe», он стал рассылать его знакомым в качестве шутки. После того как хакер убедился, в том, что способен заставить чужие компьютеры выполнять требумые действия, он написал «скрытый майнер» - программу, которая должна была генерировать для него биткойны на зараженных ПК.

Когда майнер был готов, молодой человек замаскировал его под другое программное обеспечение и залил на файлообменник cloud.mail.ru. Ссылку на скачивание своей программы он раскидал на тематических форумах, введя пользователей в заблуждение. Оставалось только ждать богатства.

Но дождаться желанного богатства компьютерному гению не удалось – правоохранители вышли на него в связи с делом, возбужденным по заявлению пострадавшей блогерши, кража Instagram-аккаунта которой стала его первым криминальным «крещением».

Изъяв компьютерную технику, полицейские распутали весь последующий клубок преступных деяний, в результате чего, к первоначальному обвинению в несанкционированном взломе компьютерных систем (ст. 361, УКУ), добавились аналогичные, совершенные повторно, что лишь усугубило вину подозреваемого.

Полностью признав свою вину, обвиняемый заключил соглашение с Прокуратурой, в результате которого 2 года заключения были заменены на условный срок с испытательным периодом и обязательной постановкой на учет и посещением органа пробации по месту проживания». ***(Андрей Майданик. Украинский хакер получил 2 года за добычу Bitcoin на чужих компьютерах // Internetua (https://internetua.com/ukrainskii-haker-polucsil-2-goda-za-dobycsu-bitcoin-na-csujih-kompuaterah). 25.01.2021).***

***

«Хакери за допомоги вірусного програмного забезпечення здійснювали масові втручання в роботу серверів приватних та державних установ країн Європи та Сполучених Штатів Америки. У результаті такої «діяльності» іноземним банкам та фінустановам нанесено 2,5 мільярда доларів збитків. Зловмисникам загрожує до дванадцяти років ув’язнення.

У рамках міжнародної спецоперації Департаменту кіберполіції спільно з Головним слідчим управлінням Нацполіції, Офісом Генерального прокурора України, із залученням колег з правоохоронних органів Німеччини, США, Великобританії та Нідерландів, було викрито та заблоковано діяльність транснаціонального хакерського злочинного угруповання з розповсюдження найнебезпечнішого і найстійкішого вірусного програмного забезпечення – «EMOTET».

Інфраструктура «EMOTET» включала сервери, розташовані по всьому світу, і фактично була БОТ-мережею. «Вірус» поширювався шляхом спам-розсилок, через документи Word, Excel тощо. Електронні листи виглядали як попередження про

безпеку облікового запису, запрошення на вечірку і навіть як застереження від поширення COVID-19.

Проникнувши у програмне забезпечення, вірус використовував «інфіковану» техніку для подальшої розсилки, а також встановлював на пристрій додаткові віруси. У результаті шкідливе програмне забезпечення викрадало персональні дані користувачів, зокрема паролі, логіни, історію браузера, платіжні та банківські дані тощо. У подальшому зловмисники перераховували гроші на свої підконтрольні рахунки.

Під час слідчих дій встановлено двох громадян України, які забезпечували належну роботу інфраструктури розповсюдження вірусу та підтримували його безперебійну діяльність.

Перший заступник начальника Департаменту кіберполіції Сергій Кропива повідомив: «Локомотивом проведення операції виступають українські правоохоронці, а роль координаторів виконують Європол та Євроюст. На даний час підтверджено, що вірус завдав збитків банкам і фінансовим установам США та Європи на 2,5 мільярда доларів».

Кіберполіцейські спільно з правоохоронцями іноземних держав одночасно провели обшуки на території України, Нідерландів, Німеччини, Франції, Литви, Канади, США та Великобританії. За результатами вилучено серверне обладнання, комп’ютерну техніку, носії інформації, що містять відомості про компанії, на які здійснювалися кібератаки. Також вилучено банківські картки, гроші, «чорнові» записи з паролями, логінами та ключами до закриптованих сервісів. Наразі повністю заблоковано діяльність БОТ-мережі «EMOTET», яка розташовувалася на більш ніж 90 серверах у різних країнах світу.

Розслідується кримінальне провадження за ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку), ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів), та за ст. 190 (Шахрайство) Кримінального кодексу України. Зловмисникам загрожує позбавлення волі на строк до дванадцяти років з конфіскацією майна.

Також встановлено інших учасників міжнародного хакерського угруповання, які використовували інфраструктуру БОТ-мережі «EMOTET» для проведення кібератак. Проводяться заходи для їх затримання». ***(Кіберполіція викрила транснаціональне угруповання хакерів у розповсюдженні найнебезпечнішого в світі комп’ютерного вірусу «EMOTET» // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-transnaczionalne-ugrupovannya-xakeriv-u-rozpovsyudzhenni-najnebezpechnishogo-v-sviti-kompyuternogo-virusu-emotet-2504/). 27.01.2021).***

***

«Фігуранти в Інтернеті збували дані про перетин українського кордону громадянами та транспортними засобами. Зловмисники продавали вже сформовані бази та приймали замовлення на створення нових. Їм загрожує до п’яти років ув’язнення.

Правопорушення викрили співробітники кіберполіції Івано-Франківщини спільно зі слідчими Косівського відділу поліції та працівниками обласного управління внутрішньої безпеки Нацполіції.

Кіберполіція встановила, що до несанкціонованого збуту інформації причетні двоє 30-річних чоловіків – мешканці Тернопільської та Івано-Франківської областей. Фігуранти в Інтернеті, зокрема на платформах оголошень, пропонували до купівлі бази даних про перетин державного кордону України. У розпорядженні зловмисників були відомості щодо перетину кордону українськими та іноземними громадянами, транспортними засобами, а також терміни їхнього перебування в країні.

Коштувала одна сформована база від 500 до 1500 гривень. Також правопорушники працювали «на замовлення».

Правоохоронці провели обшуки в оселях фігурантів. За результатами вилучено мобільні телефони, банківські карти та комп’ютерну техніку.

Наразі поліцейські перевіряють працівників митної та прикордонної служби України на причетність до незаконного розповсюдження інформації з обмеженим доступом.

Фігурантам оголошено підозру за ч. 2 ст. 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в комп'ютерах, автоматизованих системах, комп'ютерних мережах) Кримінального кодексу України. Санкція статті передбачає до п’яти років позбавлення волі. Досудове слідство триває.

Процесуальне керівництво у справі здійснює Косівський відділ Коломийської місцевої прокуратури. Слідчі дії проводилися спільно з працівниками СБУ в Івано-Франківській області». ***(Кіберполіцейські викрили двох осіб у незаконному збуті інформації про перетин державного кордону України // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpoliczejski-vykryly-dvox-osib-u-nezakonnomu-zbuti-informacziyi-pro-peretyn-derzhavnogo-kordonu-ukrayiny-8221/). 28.01.2021).***

***

«Служба безпеки України протягом 2020 року нейтралізувала 600 кібератак на інформаційні ресурси органів влади та об’єкти критичної інфраструктури.

…про це йдеться у повідомленні СБУ.

Наголошується, що за цей період нейтралізовано 20 угруповань, причетних до багатьох кібератак, а також заблоковано понад 2,6 тис. спільнот з мільйонною аудиторією та 21 бот-мережу потужністю близько 60 тисяч акаунтів.

«Завдяки роботі кіберфахівців СБУ до кримінальної відповідальності за поширення антиукраїнської пропаганди було притягнуто 40 осіб і ще 32 фігурантів вже засуджено. В’їзд на територію України заборонено 158 іноземцям, котрі причетні до пропаганди сепаратизму в інтернеті», - поінформували у спецслужбі.

Крім того, в рамках протидії несанкціонованим втручанням у роботу комп’ютерів та автоматизованих мереж співробітники СБУ викрили схему, яка завдавала масштабних збитків економіці держави. «Її організувало колишнє

керівництво Державної податкової служби. Так, збитки державі через різні податкові «скрутки» і конвертцентри оцінюються у 35 млрд гривень», - зазначається в повідомленні.

Кіберфахівці СБУ також викрили шість злочинних груп, які незаконно втручалися у бази даних Мін'юсту і вносили в державні реєстри недостовірну інформацію.

Загалом протягом 2020 року за матеріалами кіберпідрозділів СБУ розпочато 496 кримінальних проваджень. Із них – 129 справ саме за несанкціоноване втручання у роботу комп'ютерних мереж та автоматизованих систем.

Також за ініціативи СБУ було продовжено санкції стосовно низки російських сайтів і програмних продуктів. Окремо спецслужба направила звернення до компаній Google та Apple щодо блокування заборонених російських додатків на їхніх електронних майданчиках». ***(СБУ торік нейтралізувала 600 кібератак // Укрінформ (https://www.ukrinform.ua/rubric-society/3174901-sbu-torik-nejtralizuvala-600-kiberatak.html). 21.01.2021).***

***

«Киберспециалисты ГУ СБУ в Киеве и Киевской области в прошедшем году нейтрализовали 154 кибератаки и киберинцидентов на информационные ресурсы органов власти и объекты критической инфраструктуры. Оперативники СБУ также блокировали деятельность 4 хакеров, которые действовали по заданию спецслужб РФ.

Об этом KV стало известно из сообщения пресс-службы ГУ СБУ в Киеве и Киевской области.

За год СБУ прекратила в Киеве деятельность 65 интернет-платформ, которые действовали в ущерб государственной безопасности, разоблачила 144 факта использования электронных кошельков и аккаунтов, в том числе для финансирования так называемых "Л/ДНР" и международного терроризма.

Также спецслужба запретила въезд в Украин 4 иностранцам, которые через соцсети распространяли антиукраинской контент и поддерживали военную агрессию РФ против Украины. За действия в ущерб информационной безопасности Украины объявлено 16 официальных предостережений…». ***(Более полутора сотен угроз нейтрализовали сотрудники кибербезопасности столичной СБУ в 2020 году // Интернет-издание «КиевВласть» (https://kievvlast.com.ua/news/bolee-polutora-soten-ugroz-nejtralizovali-sotrudniki-kiberbezopasnosti-stolichnoj-sbu-v-2020-godu). 22.01.2021).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Глобальная пандемия COVID-19 по-прежнему имеет серьезные и далеко идущие последствия для отдельных лиц, а также организаций и предприятий по всему миру по разным причинам. Одним из последствий стало

усиление обеспокоенности, связанной с кибербезопасностью и защитой данных, в различных областях, некоторые из которых, вероятно, станут ключевыми областями внимания в ближайшие месяцы.

Одной из важных проблем является тот факт, что, как сообщается, киберпреступники и предполагаемые государственные хакеры одинаково атакуют системы здравоохранения, и эта проблема, вероятно, усугубится в результате реализации крупных программ вакцинации COVID-19 по всему миру.

Глобальная цепочка поставок таких вакцин сложна и часто включает в себя различные элементы в ряде разных стран, при этом в некоторых юрисдикциях уже отмечены случаи, когда киберпреступники пытаются по-разному нарушить цепочки поставок вакцин. Это означает, что при распространении вакцин COVID-19 могут возникнуть проблемы с кибербезопасностью.

Еще одна проблема, вызывающая беспокойство, - это целенаправленность исследований вакцин. Хакеры, нацеленные на такие исследования, не обязательно сосредоточены на получении личных данных, но могут, среди прочего, пытаться продвигать разработки в других юрисдикциях или получить интеллектуальную собственность для получения коммерческой выгоды. Другие проблемы включают дискредитацию данных испытаний и безопасности страны, а также распространение неточной информации о вакцинах в Интернете.

Однако атаки программ-вымогателей, особенно в больницах, по-видимому, продолжают оставаться наиболее серьезной проблемой кибербезопасности, особенно те, которые препятствуют оказанию помощи пациентам. Как отмечается в этой статье, оцифровка здравоохранения была ускорена COVID-19, и теперь используется гораздо больше инструментов и систем, подключенных к Интернету, чем раньше.

Это привело к опасениям, что киберпреступники могут сместить акцент с отказа организациям в доступе к их медицинской информации на активное вмешательство в нее, что может создать риски для безопасности пациентов.

Чтобы попытаться решить эти проблемы, соответствующие организации в Великобритании должны убедиться, что они соблюдают все применимые требования кибербезопасности, включая (среди прочего) обязательства, включенные в Общий регламент Великобритании по защите данных (UK GDPR) и Закон Великобритании о защите данных. 2018 в отношении безопасности личных данных.

Британским организациям также может потребоваться соблюдение требований Общего регламента по защите данных (ЕС) 2016/679 (ЕС GDPR) в той степени, в которой они либо предлагают товары или услуги субъектам данных в ЕС, либо отслеживают поведение субъекты данных в ЕС.

Соответствующие британские организации также должны убедиться, что они соблюдают требования Регламента по сетям и информационным системам 2018 (SI 2018/506), (Правила NIS), которые налагают различные обязательства по кибербезопасности и отчетности об инцидентах на соответствующих поставщиков цифровых услуг и операторов основных услуг. которые работают в определенных секторах (включая здравоохранение) и соответствуют пороговым рабочим

требованиям. Правила NIS сосредоточены на безопасности ИТ-систем, а не на безопасности личных данных, обрабатываемых этими системами.

Все эти риски означают, что в будущем для организаций и предприятий, вовлеченных в сектор здравоохранения, будет как никогда важно предпринять решительные шаги по обеспечению безопасности своих ИТ-систем и устройств, чтобы попытаться обеспечить, чтобы общественное здравоохранение и отдельные пациенты безопасность защищена насколько это возможно». ***(Clare Sellars. Cybersecurity threats to healthcare due to COVID-19 set to increase // Ropes & Gray (https://ropesgrayinsights.passle.net/post/102goaq/cybersecurity-threats-to-healthcare-due-to-covid-19-set-to-increase). 08.01.2021).***

***

«Организация признала, что хакеры слили украденную информацию о вакцинах от COVID-19 в рамках кибератаки, нацеленной на медицинское агентство Европейского Союза.

Атака на Европейское агентство по лекарственным средствам (EMA) впервые была раскрыта в прошлом месяце, и теперь установлено, что те, кто стоит за взломом, получили доступ к информации о лекарствах от коронавируса.

«Продолжающееся расследование кибератаки на EMA показало, что некоторые незаконно полученные документы, связанные с лекарствами от COVID-19 и вакцинами, принадлежащими третьим лицам, были просочены в Интернет. Правоохранительные органы принимают необходимые меры», - сообщает EMA говорится в заявлении.

«Агентство продолжает полностью поддерживать уголовное расследование по факту утечки данных и уведомлять любые дополнительные юридические и физические лица, чьи документы и личные данные могли быть объектом несанкционированного доступа», - добавило EMA.

На работу EMA и европейскую сеть регулирования лекарственных средств это нарушение не повлияло, а утверждение и распространение вакцин против COVID-19 не было нарушено.

Предыдущее обновление показало, что хакеры получили доступ к информации, нарушая один нераскрытый ИТ приложений - и что нападавшие были специально нацеленные данные, связанные с COVID-19 лекарств и вакцин. Расследование нападения все еще продолжается…». ***(Danny Palmer. Hackers have leaked the COVID-19 vaccine data they stole in a cyberattack // ZDNet (https://www.zdnet.com/article/hackers-have-leaked-the-covid-19-vaccine-data-they-stole-in-a-cyberattack/). 13.01.2021).***

***

«Эксперты по безопасности и правительственные чиновники готовятся к волне кибератак, направленных на процесс распространения вакцины от коронавируса.

Сложная цепочка поставок, стоящая за производством и доставкой вакцин, создает множество возможностей для хакеров. Атаки могут исходить от хакеров-преступников, мотивированных финансовыми стимулами, или со стороны

национальных государств, стремящихся вызвать экономические и гражданские потрясения.

«Нам нужно подумать о том, насколько велика эта поверхность атаки - она будет становиться все больше и больше», - говорит Ник Россман, руководитель отдела глобальной аналитики угроз в IBM Security X-Force, которая отслеживает кибератаки, связанные с коронавирусом, с начала пандемии.

Он видел, как хакеры развиваются вместе с пандемией, в последнее время обращаясь к атакам на процесс доставки вакцин от производителей к пользователям. Его команда в прошлом месяце сообщила о фишинговой кампании государственных субъектов, нацеленной на компании, участвующие в той части цепочки поставок, которая поддерживает вакцины при соответствующей температуре.

«Мы наблюдаем эту продолжающуюся кампанию против цепочки поставок, в частности, - сказал Россман. Теперь хакеры изучают «компании или организации, которые, возможно, не вкладывали много средств в безопасность, но сейчас находятся в авангарде распространения», - говорит он.

Гонка за прекращение пандемии имеет огромные экономические и геополитические последствия. Национальные государства, стремящиеся нанести ущерб Соединенным Штатам, могут нарушить процесс распространения вакцины как средство ослабления их глобального положения.

Цели включают больницы.

Во время пандемии количество атак программ-вымогателей на больницы неуклонно растет. Хакеры используют эту форму атаки, чтобы взять под контроль систему организации, пока она не выплатит выкуп.

Даже если хакеры не хотят намеренно вмешиваться в распространение вакцины, они могут извлечь выгоду из того давления, которое испытывают больницы из-за коронавируса.

«Давление, заставляющее их вернуться к работе, заставляет их с большей готовностью платить, чем некоторые другие цели, - говорит Марк Роджерс, вице-президент по кибербезопасности Okta. Он также является соучредителем CTI League, группы профессионалов-добровольцев со всего мира, работающих над борьбой с кибератаками против организаций здравоохранения.

Представители службы кибербезопасности США находятся в состоянии повышенной готовности к атакам на цепочки поставок.

Агентство по кибербезопасности и безопасности инфраструктуры отслеживает изменения в потенциальных угрозах, вызванных распространением вакцины, говорит Джош Корман, главный стратег агентства по здравоохранению и covid-19.

CISA следит за активными угрозами противодействия коронавирусу с момента начала пандемии. Первоначально агентство сосредоточило свои усилия на первых объектах хакеров: ведущих фармацевтических компаниях, исследовательских организациях и нескольких десятках компаний, поддерживающих их функции.

Сейчас CISA работает над предоставлением рекомендаций по кибербезопасности и физическим угрозам для широкого круга организаций с

сильно различающимися уровнями безопасности. По словам Кормана, поскольку протоколы распределения вакцин варьируются от штата к штату, правила CISA постоянно развиваются вместе с изменениями в этих процедурах.

Как исследователи, так и правительственные чиновники следят за угрозами со стороны субъектов национального государства.

Администрация Байдена призвала Управление директора национальной разведки оценить «текущие киберугрозы и кампании иностранного вмешательства, направленные на вакцины против COVID-19 и связанные с ними меры общественного здравоохранения», в плане реагирования на пандемию, опубликованном на прошлой неделе.

В ODNI отказались от дальнейшего обсуждения работы.

«DNI стремится предоставлять лучшие идеи [разведывательного сообщества] и оказывать поддержку политикам и стране в этом вопросе», - говорится в заявлении представителя ODNI.

Кибератаки иностранных злоумышленников в начале пандемии были сосредоточены на шпионаже и краже исследований. Летом США обвинили Китай и Россию в попытке украсть исследования коронавируса.

Эти усилия будут продолжаться по мере того, как производители вакцин будут разрабатывать новые версии своих лекарств. Но теперь к этой смеси добавляются атаки на цепочки поставок, направленные на создание экономической и гражданской нестабильности в США, предупреждают эксперты.

«Страны, стремящиеся дестабилизировать другие страны, будут стремиться сорвать этот процесс». - говорит Роджерс.

Плохие участники могут также использовать атаки, чтобы вызвать дезинформацию и замешательство.

Европейское агентство по лекарственным средствам вчера сообщило, что взлом документов, связанных с пандемией, привел к подтасовке и разглашению неконтекстных версий документов «таким образом, что это может подорвать доверие к вакцинам». Эксперты предупреждают, что кибератаки против цепочки поставок в США могут иметь аналогичные результаты.

Любая атака на цепочку поставок может иметь разрушительные и смертельные последствия.

По словам Кормана, хакеры-преступники, стремящиеся быстро заработать на последней стадии борьбы с пандемией, могут быть более небрежными, чем «осторожные, талантливые» субъекты национального государства. Это может привести к непреднамеренно разрушительным последствиям; даже финансово мотивированные нападения могут привести к сбоям в работе, что приведет к экономическим потрясениям и человеческим жертвам.

«Злоумышленники [например, хакеры-преступники] могут не желать причинять смерть людям или нарушать национальную безопасность, но даже что-то вроде программ-вымогателей может иметь невероятные последствия», - говорит Корман. Он указал на последствия атаки России на энергосистему Украины в 2017 году, в результате которой промышленным предприятиям по всему миру был нанесен ущерб на миллиарды долларов.

«Злонамеренный умысел не является предпосылкой причинения вреда»

Задержка с распространением может резко увеличить число погибших от пандемии в Соединенных Штатах, добавил Корман. Более 419000 американцев умерли от коронавируса.

Партнерство между частным сектором и правительством могло бы усилить защиту.

И Корман, и Роджерс указали на необходимость более тесного партнерства между частным сектором и правительством для защиты от атак на цепочки поставок.

«Мы далеко не из леса», - говорит Корман». ***(Tonya Riley. The Cybersecurity 202: Vaccine distribution unleashes new cybersecurity risks // The Washington Post (https://www.washingtonpost.com/politics/2021/01/26/cybersecurity-202-vaccine-distribution-unleashes-new-cybersecurity-risks/). 26.01.2021).***

***

«Европейское агентство по лекарственным средствам (EMA) заявило в понедельник, что утечка данных о коронавирусе, циркулирующих в Интернете, «могла быть вырвана из контекста», чтобы посеять недоверие к процессу утверждения вакцин в ЕС.

EMA в декабре показало, что его системы были взломаны, а информация о вакцине от коронавируса BioNTech / Pfizer была «незаконно доступна» в ходе атаки. После того, как документы просочились в Интернет, в начале этого месяца было заявлено, что хакеры «манипулировали» информацией в документах, которые они получили в результате кибератаки, а затем просочились на форумы в темной сети.

«Более тщательное исследование опубликованных материалов показало, что не все документы были опубликованы в их целостной, оригинальной форме и, возможно, были вырваны из контекста», - говорится в сообщении агентства в понедельник.

EMA столкнулось с тщательной проверкой того, как оно сообщало о взломе. Несколько СМИ сообщили, что документы показывают, что Европейская комиссия оказала давление на агентство, чтобы ускорить процесс утверждения вакцин, но агентство не ответило на вопросы о содержании онлайн-документов.

В своем последнем обновлении он не отклонил эти обвинения напрямую, но сказал, что хакеры отредактировали информацию до ее утечки: «Хотя отдельные электронные письма являются подлинными, данные от разных пользователей были отобраны и агрегированы, были созданы скриншоты из нескольких папок и почтовых ящиков, а также были созданы дополнительные преступники добавили названия таким образом, чтобы подорвать доверие к вакцинам», - говорится в сообщении…». ***(LAURENS CERULUS. EU medicines agency says hackers manipulated leaked coronavirus vaccine data // POLITICO (https://www.politico.eu/article/european-medicines-agency-ema-cyberattack-coronavirus-vaccine-data/). 25.01.2021).***

***

«Продовжується Всесвітній економічний форум у Давосі, який цього року проходить в онлайн-форматі. Одними із найважливіших тем для обговорення стали проблема боротьби з пандемією, економічне відновлення після коронавірусної кризи та загроза кліматичних змін.

Пандемія COVID-19 різко збільшила залежність економіки та суспільства від цифрових технологій, тим самим поглибивши вразливість людей, підприємств та урядів до кібератак. Саме проблема кібербезпеки стає однією з ключових на тлі активного розвитку та впровадження цифрових технологій у життя людей, вважають спікери форуму в Давосі. Людство ризикує стати жертвою так званої «кіберпандемії».

Пандемія коронавірусу дестабілізувала економіку та людське суспільство, продемонструвавши те, наскільки вразливими є люди до біологічних загроз. У цифровому світі також існують подібні ризики, які загострилися саме зараз, адже останнім часом кібератаки почали поширюватися так само, як вірус у реальному світі.

«Вже неодноразово згадувалося, що COVID-19 неабияк прискорив діджиталізацію. Саме технології допомагали людям підтримувати зв'язок під час дії карантинних обмежень. Все це спровокувало надмірну залежність людства від цифрових технологій. Цілком очікуваним стало те, що зросла кількість кібератак. Саме тому політика урядів країн щодо цифрового простору повинна трансформуватися, адаптуватися до всіх змін», - каже представник Агенції кіберпезпеки Сінгапуру Девід Коі. За його словами, пандемія коронавірусу спровокувала колапс у реальному світі, тоді як кіберпандемія ризикує спровокувати кризу в цифровому світі.

На думку Девіда Коі, у випадку з кіберпандемією, так само як і у випадку з пандемією коронавірусу, важливою є глобальна співпраця та розуміння спільної відповідальності. Для того, щоб захистити себе від кіберзагроз різні сектори економіки повинні співпрацювати.

Окрім глобальної співпраці, уряди країн можуть створювати власні національні стратегії з досягнення кібербезпеки, адже ключові елементи урядових інфраструктур знаходяться під загрозою хакерських атак, яскравим прикладом цього були недавні хакерські атаки на урядові відомства США…» ***(Давоський форум-2021: розвиток технологій може спровокувати початок «кіберпандемії» // Дзеркало тижня. Україна (https://zn.ua/ukr/WORLD/davoskij-forum-2021-rozvitok-tekhnolohij-mozhe-sprovokuvati-pochatok-kiberpandemiji.html). 28.01.2021).***

***

Світові тенденції в галузі кібербезпеки

«Основные технологические тенденции в юридической профессии на 2021 год, вероятно, будут включать в себя искусственный интеллект, цепочку блоков и криптовалюты, автономные транспортные средства, цифровое здравоохранение и… судебные документы на бумаге. После недавнего широко распространенного нарушения кибербезопасности федеральные суды Соединенных

Штатов запрещают электронную регистрацию строго конфиденциальных документов. Стороны должны хранить такие документы на бумаге или в виде электронных файлов на защищенном электронном устройстве.

В середине декабря Агентство по кибербезопасности и безопасности инфраструктуры (CISA) Министерства внутренней безопасности (DHS) издало чрезвычайную директиву, раскрывающую кибератаку в сетях местных, государственных и федеральных агентств, а также частных компаний. По словам CISA, вредоносные актеры эксплуатировали Orion Solarwinds' ®исходный код продукта для взлома этих сетей. (SolarWinds описывает Orion как «мощную масштабируемую платформу для мониторинга и управления инфраструктурой, разработанную для упрощения ИТ-администрирования для локальных, гибридных сред и сред «программное обеспечение как услуга» (SaaS) в единой панели».) Ранее на этой неделе United Спецслужбы штатов, в том числе ФБР, АНБ и Управление директора национальной разведки, заявили, что нападение "вероятно, было русским по происхождению". В ответ на кибератаку суды Соединенных Штатов приостановили все использование SolarWinds Orion на национальном и местном уровнях.

Кибератака, по-видимому, скомпрометировала сетевую инфраструктуру Административного управления судов США, агентства, которое разработало и поддерживает систему управления делами и электронной судебной документации, известную как CM / ECF (Управление делами / Электронные файлы дел) («Административный офис»). В 1996 году Северный округ штата Огайо был первым федеральным судом, внедрившим систему CM / ECF. С тех пор более двухсот судов США приняли систему CM / ECF, позволяющую сторонам подавать документы в электронном виде, а публике - просматривать судебные документы.

В большинстве дел о патентах и коммерческой тайне - а также во многих сложных коммерческих делах - стороны добиваются внесения в суд постановления о защите, регулирующего производство и разглашение коммерческой тайны, конфиденциальных документов и другой информации. Чтобы продвигать общую политику в пользу предоставления публичного доступа к судебным записям, большинство документов становятся общедоступными. Документы, которые содержат действительно секретную или конфиденциальную информацию, обычно хранятся и хранятся за печатью, часто с отредактированными версиями, хранящимися в общедоступных записях по делу. Следовательно, то, что хранится за печатью, часто содержит наиболее строго охраняемую техническую, финансовую или личную информацию сторон, публичное раскрытие которой может иметь потенциально катастрофические последствия для сторон, предоставивших такую информацию.

Федеральные агентства в настоящее время проводят аудит безопасности своих систем, чтобы определить степень и влияние атаки. Административный офис оценивает уязвимости в системе CM / ECF, которые раскрывают или потенциально раскрывают конфиденциальные или конфиденциальные документы, хранящиеся за печатью. Между тем, новые процедуры, объявленные административным офисом 6 января 2021 года, предусматривают, что высокочувствительные документы (HSD), поданные в суды США, должны быть представлены на бумаге или в виде файлов,

загруженных на защищенные электронные устройства, такие как USB-накопители, которые будут храниться на безопасная автономная компьютерная система в соответствующем суде. Отдельные суды должны применять свои собственные местные процедуры, регулирующие такие обращения…

Хотя в 2021 году в юридической профессии, вероятно, будут преобладать новые и передовые технологии, могут появиться некоторые передовые методы, позволяющие избегать использования технологий для обеспечения защиты конфиденциальной информации клиентов. Так и с бумагой: то, что было старым, снова становится новым». ***(David Prueter, David Elkins. What Was Old Is New Again In IP Litigation — Thanks To Suspected Russian State-Sponsored Hack // Global IP & Technology Law Blog (https://www.iptechblog.com/2021/01/what-was-old-is-new-again-in-ip-litigation-thanks-to-suspected-russian-state-sponsored-hack/#page=1). 08.01.2021).***

***

«Люди в организации часто являются первой и передовой линией защиты кибербезопасности. В кругах кибербезопасности существует тенденция сосредотачиваться на технологических и инфраструктурных решениях, системах и процессах для поддержания безопасности. Это критически важно. Однако не менее, если не более важно, люди в организации. Это люди, которые управляют существующими системами, следят за процессами и в целом ведут бизнес.

Качество программ обучения и повышения осведомленности будет иметь прямое положительное влияние на сокращение утечек данных и смягчение неблагоприятных последствий утечек данных, когда они действительно происходят. Эффективное обучение повысит осведомленность об угрозах информационной безопасности в бизнесе, о том, как сообщать об инцидентах и как играть роль в реагировании на инциденты и утечки данных. Это, в свою очередь, снижает и сокращает убытки и ответственность, возникающие в результате утечки данных.

Отсутствие эффективного обучения - частая критика в отчетах регулирующих органов о серьезных нарушениях данных. Это подчеркивает, что эффективное обучение кибербезопасности является ожидаемым стандартом для бизнеса. Отсутствие эффективной программы обучения будет неблагоприятным и отягчающим фактором в расследованиях и судебных разбирательствах, проводимых регулирующими органами, когда происходит утечка данных.

Кого следует обучать

Любой, кто участвует в ведении бизнеса, должен быть обучен в отношении угроз безопасности, исходящих от этого бизнеса. Обучение должно быть адаптировано к роли и функциям обучаемых, чтобы обучение было актуальным и связанным. Даже люди, которые не имеют постоянного или какого-либо доступа к ИТ-системам, должны пройти определенную подготовку, хотя контент будет адаптирован с учетом физической безопасности или других мер, относящихся к их конкретной роли. Обучение не может быть ограничено только сотрудниками и

может включать подрядчиков, поставщиков и других лиц, имеющих доступ к бизнес-помещениям или ИТ-системам.

Обучение должно подчеркивать роль каждого человека в поддержании конфиденциальности, целостности и доступности данных и информации о бизнесе. Обучение должно помочь людям выявлять угрозы информационной безопасности и действиям, которые следует предпринять, если они выявляют угрозы или инциденты.

Когда следует проводить обучение

Тренировки должны быть рассчитаны по-разному, чтобы разнообразить программу тренировок. Это может включать:

Индукционная: Кибербезопасность обучение должно быть ключевым компонентом программы индукции. Это поможет привить передовой опыт с самого начала и снизить вероятность формирования вредных привычек с самого начала.

Запланировано: некоторые основные темы должны рассматриваться часто и периодически. Это служит постоянным напоминанием об общих и постоянных угрозах информационной безопасности. Хороший тому пример - повторное обучение фишинговым атакам.

По запросу: определенное обучение должно быть доступно на основе «всегда в наличии, по запросу». Это позволяет занятым людям знакомиться с соответствующими учебными темами и материалами в удобное для них время.

Точно в срок: определенное обучение может быть предоставлено «точно в срок». Это может возникнуть, если обучение проводится непосредственно в сочетании с конкретным процессом, который требует такого обучения, или в определенный период, когда эта угроза наиболее высока. Например, обучение кибербезопасности в период рождественских праздников является примером предоставления обучения, совпадающего с периодом повышенного риска кибербезопасности.

Сюрприз: обучение может быть наиболее эффективным, если оно проводится в неожиданное время. Это подчеркнет реальный уровень осведомленности людей по предмету. Например, смоделированная фишинговая атака покажет, как люди отреагировали на фишинговую атаку, и предоставит достоверные данные и действия, основанные на реакции людей.

Ловушка, которой следует избегать, состоит в том, чтобы строго придерживаться годового календаря, который требует, чтобы участники набрали определенное количество учебных часов в течение этого периода. Это неизбежно приводит к отсутствию обучения в течение большей части года и спешке за получением кредитов на обучение в сумерках этого периода. Неизбежно страдает качество обучения и уровень обучения.

Формы обучения

Форма и метод обучения должны быть разнообразными. Некоторые стили включают:

Лекция: это традиционный формат лекции, в котором преподаватель доставляет содержание непосредственно обучающимся. Это может быть доставлено в реальной или онлайн-среде. Могут использоваться вспомогательные средства презентации, такие как слайд-колода, анкеты участников или опросы.

Этот традиционный стиль требует от участника большей сосредоточенности и выносливости, чтобы оставаться вовлеченным и набирать очки обучения. Это может быть полезно на вводном уровне или как основная презентация по теме для дальнейшего использования.

Семинар: это более интерактивный формат, в котором тема обучения изучается в небольшой группе. Как правило, используется сократический стиль преподавания, при котором преподаватель напрямую задает вопросы участникам или разбивает группу на более мелкие рабочие группы по задачам или решению проблем, связанных с темой. Это эффективный метод поощрения самообучения за счет выполнения задач или решения проблем.

Круглый стол: в этом формате тренер ведет дискуссию между участниками, чтобы изучить тему тренинга. Это эффективный метод, в котором желаемой целью является обмен опытом и получение новых идей из этого опыта. Он часто используется людьми, которые работают в разных отделах или функциях, но разделяют общие проблемы. Это также может быть очень эффективным среди руководителей высшего звена.

Настольные симуляции: в этом формате инструктор проведет небольшую кросс-функциональную группу через различные этапы симулированного инцидента. Цель упражнения - оценить знания и готовность участников в контексте реального происшествия и выявить слабые места в их реакции. Это особенно эффективно при обучении групп реагирования на инциденты.

Информационные программы

Программы повышения осведомленности очень важны для внедрения культуры безопасности в организацию. Осведомленность отличается от тренировки. Обучение носит направленный характер и ориентировано на конкретное обучение по конкретным темам. Осведомленность - это использование окружения людей и привлечение их внимания, чтобы они осознавали важность и актуальность информационной безопасности в организации. Это можно сделать с помощью кампаний, мультимедийных сообщений, напоминаний и любого количества творческих или новаторских мероприятий.

Ключевыми составляющими успеха информационных программ являются разнообразие и неожиданность. После того, как плакат какое-то время висит на стене в кладовой, он, кажется, становится частью стены и становится почти невидимым. В программе повышения осведомленности должен быть элемент неожиданности и веселья, который в конкретный момент ставит во главу угла информационную безопасность.

Ключевые ингредиенты для эффективной программы тренировок

Ключевыми составляющими эффективной программы обучения в области кибербезопасности и реагирования на утечки данных являются:

Поддержка высшего руководства: программа обучения должна быть утверждена и поддержана высшим руководством. Это мощный сигнал о важности обучения, когда высший руководитель - в идеале генеральный директор - активно участвует в программе обучения и в своих сообщениях постоянно подчеркивает важность обучения кибербезопасности. Поддержка высшего руководства также означает поддержку бюджета.

Организационное участие: программа обучения - это не вопрос только отдела обучения. Основная цель обучения - актуальность. Это требует активного участия на межведомственной, межфункциональной основе. Это очень важно на этапе планирования, так как именно на этом этапе цель обучения адаптируется к конкретным потребностям конкретных участников.

Измерение эффективности: обучение - это не только показ; это об извлечении практических уроков. Программа обучения должна включать способы оценки и измерения того, были ли достигнуты цели обучения. Это можно измерить с помощью инструментов оценки, таких как анкеты и формы обратной связи, или более сложных инструментов внимания для онлайн-среды.

Заключительные мысли

Овощи. Мы знаем, что они нам нужны. Но, ну, они не всегда вкусны. Обучение может быть таким. Требуется обучение. Невозможно эффективно отреагировать на утечку данных, если не было обучения тому, как это делать. Обучение - необходимый и жизненно важный компонент в реагировании на утечку данных. Мы в Tanner De Witt разработали учебные программы по защите данных и безопасности, которые помогли ряду наших клиентов.

Ключом к эффективному обучению является обеспечение разнообразия и соответствия обучению. Это требует творческих способностей, навыков планирования и исполнения. Но при организационной поддержке и участии обучение в области кибербезопасности и реагирования на утечки данных может быть четким и ярким, а не переваренным или повторным». ***(Pádraig Walsh. Data Breach Response: The importance of training // Tanner De Witt.Disclaimer (https://www.tannerdewitt.com/data-breach-training/#page=1). 08.01.2021).***

***

«Согласно прогнозам на 2021 год, внутренние угрозы будут пересмотрены в 2021 году, тенденция к работе на дому будет продолжать определять ландшафт угроз, а мобильные конечные точки станут предпочтительным вектором атаки.

После сокращения в 2020 году бюджеты на кибербезопасность в 2021 году превысят допандемические ограничения. Аутентификация, защита данных в облаке и мониторинг приложений будут первыми в списке приоритетов бюджета и кибербезопасности CISO. По мнению экспертов, это лишь некоторые из тем, которые будут доминировать в предстоящем году.

Вот круговой список экспертных заключений, освещающих предстоящий год.

Дом там, где нападения будут в 2021 году

Нет никаких сомнений в том, что ИТ-персонал все еще не оправился от массовой смены работы из дома, которая заставила их переосмыслить кибербезопасность и привела к новой зависимости от таких технологий, как облачные сервисы и цифровые инструменты для совместной работы, такие как Zoom, Skype и Slack. Эти тенденции 2020 года будут иметь длительное влияние.

Около 70 организаций, опрошенных Skybox, заявили, что более трети их сотрудников будут оставаться удаленными как минимум в течение следующих 18

месяцев. По словам генерального директора Adaptiva Дипака Кумара, в следующем году это приведет к росту защиты конечных точек. Он сообщил Toolbox Security, что защита конечных точек затронет 55% ИТ-команды, поскольку компании стремятся защитить активы, приобретенные и развернутые для удаленных сотрудников.

Исследователи Bitdefender соглашаются и говорят, что обеспечение безопасности удаленных сотрудников станет основным приоритетом для организаций. Фактически, это будет императивом, поскольку удаленные сотрудники будут продолжать предоставлять уникальный набор возможностей для плохих парней.

«Поскольку все больше и больше людей соблюдают график работы на дому, введенный пандемией коронавируса, сотрудники будут использовать ярлыки кибербезопасности для удобства», - считают исследователи Bitdefender. «Недостаточно защищенные личные устройства и домашние маршрутизаторы, передача конфиденциальной информации по незащищенным или несанкционированным каналам (таким как приложения для обмена мгновенными сообщениями, личные адреса электронной почты и облачные процессоры документов) будут играть ключевую роль в утечках и утечках данных».

Внутренние угрозы

Изменения в кадровых потребностях и продолжающаяся зависимость от удаленной рабочей силы создадут благоприятный вектор атаки для преступников, стремящихся использовать внутренние угрозы. Исследователи Forrester считают, что тенденция к удаленной рабочей силе приведет к росту внутренних угроз. Они объясняют, что уже 25 процентов утечек данных связаны с инсайдерскими угрозами, а в 2021 году ожидается, что этот процент вырастет до 33 процентов.

Forcepoint предупреждает в 2021 году о росте модели «инсайдер как услуга». Они описывают это как организованных агентов по вербовке, которые предлагают злоумышленникам целенаправленные способы стать доверенными сотрудниками для сбора конфиденциальной IP.

«Эти «плохие актеры» в буквальном смысле станут агентами под прикрытием, которые пройдут через процесс собеседования и преодолеют все препятствия, которые есть у ваших кадровых служб и служб безопасности, чтобы их остановить, - сказала Мирна Сото, директор по стратегии и доверительному управлению Forcepoint.

Входящие Bullseye

Проблемы безопасности конечных точек - одни из самых сложных сегодня и завтра. По данным анализа проблем, проведенного Crowdstrike, почтовые ящики - это щель на переднем крае защиты, часто идеальный вектор для атак программ-вымогателей, взлома корпоративной электронной почты и заражения вредоносным ПО.

В дальнейшем исследователи предупреждают, что предприятиям следует ожидать «значительного увеличения» числа целевых фишинговых атак в 2021 году из-за автоматизации.

«Киберпреступники уже начали создавать инструменты, которые могут автоматизировать ручные аспекты целевого фишинга», - заявили исследователи

WatchGuard в недавнем блоге. «Это значительно увеличит объем адресных фишинговых писем, которые злоумышленники могут отправлять одновременно, что повысит их вероятность успеха. С другой стороны, эти автоматизированные, объемные целевые фишинговые кампании, вероятно, будут менее сложными и более простыми для обнаружения, чем традиционные, созданные вручную.

Кибербезопасность Cloud Burst

Внедрение облачных технологий, вызванное пандемическими рабочими реалиями, будет только ускоряться в предстоящем году благодаря использованию программного обеспечения как услуги, процессов, размещенных в облаке, и хранилищ, которые будут стимулировать рост. Исследование Rebyc показало, что 35% опрошенных компаний заявили, что планируют ускорить миграцию рабочих нагрузок в облако в 2021 году.

Бюджетные ассигнования на облачную безопасность вырастут с однозначных до двузначных, поскольку компании стремятся защитить облачные разработки в 2020 году в предстоящем году.

Анализ Gartner приоритетов облачных вычислений на 2021 год называет «распределенное облако» приоритетным направлением деятельности предприятий, которое будет иметь серьезные последствия для безопасности. Распределенное облако - это перенос бизнес-процессов в публичное и частное облако или гибридное облако.

«[Компании] перекладывают ответственность и работу по эксплуатации аппаратной и программной инфраструктуры на поставщиков облачных услуг, используя экономику эластичности облака, извлекая выгоду из темпов инноваций, синхронизируемых с поставщиками общедоступного облака, и многое другое», - говорит Дэвид Смит, заслуженный вице-президент Аналитик Gartner.

По словам Муралидхарана Паланисами, директора по решениям в AppViewX, эта смена будет способствовать управлению облачной безопасностью (CSPM) в 2021 году. CSPM включает в себя обнаружение неправильно настроенного сетевого подключения, оценку риска данных, обнаружение либеральных разрешений для учетных записей, облачный мониторинг нарушений политики, автоматическое обнаружение и исправление неправильной конфигурации, а также соблюдение нормативных требований GDPR, HIPAA и CCPA.

Автоматизация, искусственный интеллект и машинное обучение

По словам Паланисами, защитные приложения искусственного интеллекта получат свое развитие в 2021 году, что приведет к тенденции гипер-автоматизации.

«Гиперавтоматизация - это процесс, в котором предприятия автоматизируют как можно больше бизнес-процессов и ИТ-процессов, используя такие инструменты, как искусственный интеллект, машинное обучение, роботизированная автоматизация процессов и другие типы инструментов автоматизации процессов принятия решений и задач», - сказал он.

Исследование, проведенное Splunk, показало, что 47 процентов опрошенных ИТ-руководителей заявили, что кибератаки участились с начала пандемии. Совсем недавно 36% заявили, что они столкнулись с увеличением количества уязвимостей из-за удаленной работы.

«Огромное количество предупреждений о потенциальных угрозах - это слишком много для человека, чтобы справиться с ним в одиночку. «Автоматизация и машинное обучение уже сегодня помогают аналитикам в области безопасности людей отделить самые срочные предупреждения от множества данных и принять немедленные меры по устранению определенных угроз», - написал Splunk.

В отчете признается, что осмысленное практическое применение ИИ все еще остается выходом. Но Рам Шрихарша, глава отдела машинного обучения Splunk, сказал, что «ожидает, что инструменты безопасности AI / ML будут расти в своей сложности и возможностях, как с точки зрения выявления аномалий, так и с точки зрения автоматизации эффективных контрмер».

Мобильная угроза

Мобильные угрозы усилились на фоне пандемии COVID-19, и ожидается, что эта тенденция сохранится. Угрозы варьировались от специального шпионского ПО, предназначенного для отслеживания приложений для зашифрованных сообщений, до преступников, использующих множество критических уязвимостей системы безопасности Android.

По этим причинам защитникам необходимо прислушаться к урокам прошлого года и создать программы безопасности, ориентированные на мобильные устройства, считают эксперты, мобильные устройства будут способствовать продолжающейся «де-периметризации» и облачности корпоративной сети.

«Следующим важным шагом в области безопасности является инверсия корпоративной сети», - сказал Оливер Таваколи, технический директор Vectra. «Раньше считалось, что все действительно важное хранилось на месте, и в защитной ткани проделывали небольшое количество дыр для обеспечения исходящей связи. 2021 год - это год, когда де-периметризация сети (которая давно предсказывалась), наконец, произойдет, и произойдет это с удвоенной силой. Основным показателем этого являются компании, которые отказываются от AD (устаревшая локальная архитектура) и переносят все свои удостоверения в Azure AD (современные облачные технологии)».

Как всегда, осведомленность пользователей должна быть приоритетом, по словам Билла Харрода, федерального технического директора Ivanti.

«В новую эру работы из дома мы постоянно работаем в дороге, используя целый ряд мобильных устройств, таких как планшеты и телефоны, полагаясь на общедоступные сети Wi-Fi, инструменты для удаленной совместной работы и облачные пакеты для работы», он сказал. «По мере того, как мы вступаем в новый год этой реальности, мобильные сотрудники будут представлять наибольшую угрозу безопасности, поскольку они рассматривают ИТ-безопасность как препятствие для производительности и считают, что ИТ-безопасность ставит под угрозу личную конфиденциальность».

Между тем, безопасность 5G отошла на второй план в 2021 году, хотя эти сети продолжали развиваться; но в 2021 году он вернется к разговору, потому что внедрение 5G не будет гладким.

«Когда дело доходит до внедрения всех преимуществ 5G, переход будет непростым - как для предприятий, так и для потребителей», - сказал Расс Мор, эксперт по безопасности 5G в Ivanti. «С учетом уязвимостей безопасности, которые

должны быть использованы, времени, необходимого для исправления этих уязвимостей, и постоянных развертываний протоколов, использование безопасных сетей 5G не будет беспроблемным в 2021 году». ***(2021 Cybersecurity Trends: Bigger Budgets, Endpoint Emphasis and Cloud // Threatpost (https://threatpost.com/2021-cybersecurity-trends/162629/). 03.01.2021).***

***

«NRMC возглавит усилия CISA, направленные на выявление и снижение системного киберриска

Невозможно переоценить важность передовых методов киберпространства и внедрения широко одобренных мер безопасности для защиты цифровых предприятий. Будь то программы-вымогатели, поражающие школы и больницы, или кража данных, компрометирующих конфиденциальную информацию американцев, влияние кибербезопасности - или кибербезопасности - на нашу повседневную жизнь более заметно, чем когда-либо прежде. События последних нескольких месяцев, когда субъект повышенной постоянной угрозы (APT) скомпрометировал платформу SolarWinds Orion и начал широко распространенное злоупотребление широко используемыми механизмами аутентификации, являются лишь дополнительным свидетельством этой реальности.

Мы живем в связанном мире с огромным морем информации о киберугрозах, уязвимостях и инцидентах, которые ежедневно овладевают нами. В ответ мы неуклонно углубляли партнерство между правительством и промышленностью, чтобы делиться этими точками данных на благо всех и предоставлять инструменты для повышения прозрачности и помощи в ответных действиях и усилиях по исправлению ситуации.

Это важная работа, и целостный обмен информацией, соответственно, является областью, в которую Агентство по кибербезопасности и безопасности инфраструктуры (CISA) вложило значительные средства в развитие потенциала, который мы предоставляем нашим партнерам из государственного и частного секторов.

Однако обмен информацией сам по себе никогда не станет серебряной пулей. Снижение общих киберрисков требует развитого подхода. Это требует использования существующих усилий по управлению уязвимостями, обнаружению угроз и защите сети в качестве трамплина для установления связи между угрозой, уязвимостью и последствиями с действенными метриками, которые определяют принятие решений.

В прошлом году я писал в предисловии к Руководству Национальной ассоциации корпоративных директоров по киберрискам о важности показателей киберрисков:

Несмотря на то, что это непростая задача в любом случае, необходимо приложить усилия для оценки кибервоздействия в сравнении с традиционными… метриками, а затем продвинуть анализ дальше, чтобы оценить инциденты и средства контроля с точки зрения их влияния на… результаты. Это новое мышление поможет нам лучше оценить достоинства дополнительных инвестиций в кибернетический контроль и другие формы управления рисками.

Представляем предприятие по снижению системных киберрисков

Использование передовых методов управления рисками предприятия будет в центре внимания CISA в 2021 году, и сегодня Национальный центр управления рисками (NRMC) запускает предприятие по снижению системных киберрисков, чтобы организовать нашу работу по снижению общих рисков для безопасности нации и экономической безопасности. Мы ожидаем трех всеобъемлющих направлений усилий:

Создание базовой архитектуры для анализа киберрисков критически важной инфраструктуры

Сообщество критически важной инфраструктуры поддерживается зависимой сетью оборудования, программного обеспечения, услуг и других связанных компонентов.

Возьмем, к примеру, национальную критическую функцию водоснабжения. Существует логическая иерархия способов, которыми функции (например, водоснабжение), подфункции (например, обработка загрязнения), объекты (например, муниципальное водоснабжение), активы (например, конкретный резервуар, управляемый водоканалом), включающие компоненты (например, подключенные к Интернету клапаны в резервуаре) и уязвимости на уровне компонентов (например, уязвимость промышленных систем управления в клапане) взаимодействуют и зависят друг от друга для обеспечения.

Однако в настоящее время не существует «механизма» для сбора всех этих уровней данных в инструменте динамической аналитики. Работая с отраслевыми агентствами, такими как Агентство по охране окружающей среды, NRMC в настоящее время создает Национальную архитектуру рисков для критических функций, которая будет этой движущей силой. Хотя это сложная и трудная задача, со временем эта система систем позволит нам постоянно предоставлять данные и аналитическую информацию, чтобы отвечать на ключевые вопросы управления киберрисками на основе понимания потенциального воздействия.

В конечном итоге киберриск необходимо измерять на национальном уровне с точки зрения потери функциональности. Какова вероятность того, что киберинцидент может привести к ухудшению работы системы таким образом, что функция не может быть реализована? И если эта функция не работает, каковы будут последствия с точки зрения основных приоритетов, таких как безопасность, защищенность и экономическая конкурентоспособность? Как мы можем гарантировать, что киберинциденты не могут нанести ущерб национальной безопасности? Для подобных вопросов Национальная архитектура рисков критических функций будет расширяться по модульному принципу, чтобы показать, как киберриски могут в конечном итоге проявляться в терминах функциональных последствий для критически важной инфраструктуры в масштабе. Это обеспечит более целенаправленные, приоритетные и стратегические усилия по снижению рисков и поддержит деятельность всего сообщества по лучшему пониманию непрерывности устойчивости экономики.

В 2021 году мы планируем развернуть начальную операционную возможность для этой архитектуры рисков и использовать ее для совместного принятия решений в киберпространстве на национальном уровне.

Разработка метрики киберрисков

Поддержка усилий по лучшему пониманию влияния киберрисков на сообщество критически важных инфраструктур потребует разработки пригодных для использования показателей для количественной оценки киберрисков с точки зрения функциональных потерь. Нет необходимости увязываться с греческими уравнениями с точностью до десятичных разрядов. Чрезвычайно полезны показатели, которые обеспечивают даже ориентированные или сравнительные индикаторы.

Как я упоминал ранее, цель состоит в том, чтобы лучше понять взаимосвязь между угрозой, уязвимостью и последствиями для критических функций с большей точностью, чем раньше. И воплотить это мышление в анализе затрат и выгод для снижения рисков. Для этого вам нужны метрики.

Появление рейтингов безопасности привело к количественной оценке киберрисков как способу расчета и измерения подверженности киберрискам. Эти рейтинги безопасности обеспечивают отправную точку для возможностей компаний в области кибербезопасности и помогают повысить киберриски для принятия решений советом директоров. Организации также могут использовать рейтинги безопасности наряду с метриками стратегического риска для согласования киберсценариев с существенными рисками для бизнеса; объединение киберрисков с финансовыми рисками для принятия обоснованных решений по управлению рисками; и измерить улучшение снижения киберрисков с течением времени. Такого рода работа должна происходить в зале заседаний, а также среди руководителей национальной безопасности.

Наша цель состоит в том, чтобы развить эти существующие усилия, привлечь этих партнеров и приветствовать других, которые стремятся повысить ценность этих важных обсуждений с целью добавления киберметрических показателей в пространство принятия решений в области национальной безопасности.

В ближайшие месяцы мы приступим к анализу, начнем с узких и достижимых целей, а затем расширим их.

Продвижение инструментов для борьбы с концентрированными источниками киберрисков

Центральным элементом нашего предприятия по снижению системного киберриска является поиск концентрированных источников риска, которые, если их смягчить, обеспечивают повышенную отдачу от управления рисками, если их устранить.

Пример - программный риск. Мы видели, как небезопасная цепочка поставок программного обеспечения и растущая зависимость от библиотек с открытым исходным кодом могут подвергнуть нас риску своего рода «цифровой пандемии», когда повсеместное распространение ошибок кодирования в подключенных системах создает возможность для каскадного или коррелированного воздействия на Национальные критические функции. Этот риск больше не является гипотетическим. Недостатки нулевого дня в уязвимой программной библиотеке TCP / IP Treck, выявленные в 2020 году, открыли для удаленного использования миллионы устройств Интернета вещей в различных секторах и отраслях. Соответственно, кибер-кампания SolarWinds Orion показала, как инструменты,

которые обычно используют значительное количество привилегированных учетных записей и доступ для выполнения обычных бизнес-функций, могут сами стать векторами враждебных атак, если они недостаточно усилены.

Соответственно, мы отдали приоритет программному обеспечению как области, в которой мы можем бороться с системными рисками. За последние два года мы работали через государственно-частную рабочую группу по управлению рисками цепочки поставок информационно-коммуникационных технологий (ИКТ) для выявления угроз цепочки поставок, в том числе связанных с программным обеспечением, и разработки руководств и инструментов, которые помогут компаниям ИКТ и их клиенты, включая федеральное правительство, снижают риски, связанные с цепочками поставок программного обеспечения.

CISA нацелена на то, чтобы в предстоящем году передать работу нашей целевой группы для использования в сообществе критически важной инфраструктуры, тесно сотрудничая с другими федеральными партнерами, которые активно участвовали в программе обеспечения качества программного обеспечения и спецификации программного обеспечения (SBOM). Мы изучим и другие способы снижения риска программного обеспечения, включая разработку инновационных решений, которые мы финансируем из национальных лабораторий.

Путь вперед

«Защита сегодня» и «Обеспечение завтрашнего дня» требует, чтобы мы лучше понимали и устраняли системные киберриски. Постоянный шум о важности киберпреступлений необходимо дополнить более глубоким пониманием того, как киберриски проявляются во взаимосвязанном мире - это означает как понимание взаимосвязи, так и разработку решений с высоким уровнем левериджа. CISA, используя совместный подход Национального центра управления рисками, надеется на сотрудничество с критически важной инфраструктурой и сообществом кибер-исследований, чтобы добиться прогресса в этом важном предприятии». ***(Bob Kolasky. A RISK-BASED APPROACH TO NATIONAL CYBERSECURITY // CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (https://www.cisa.gov/blog/2021/01/14/risk-based-approach-national-cybersecurity). 14.01.2021).***

***

«Согласно отчету Wandera о мобильных угрозах за 2020 год, каждую минуту в Интернете появляются три новых фишинговых сайта. Из-за пандемии и работы на дому фишинг становится популярным инструментом преступников. В апреле 2020 года Google блокировал более 18 миллионов попыток фишинга каждый день в течение недели. Это более 126 миллионов попыток фишинга за неделю. А поскольку почти все вредоносные программы (94%) доставляются по электронной почте, обеспечение того, чтобы сотрудники были киберпрограммами и хорошо обучены, должно быть высшим приоритетом для руководителей информационной безопасности (CISO) и руководителей безопасности (CSO).

Переосмыслить, как обучаются сотрудники

Традиционный корпоративный тренинг по кибербезопасности состоит из ежегодной лекции, за которой в течение года пытаются напоминать сотрудникам плакаты, электронные письма и информационные бюллетени - вещи, которые часто упускаются из виду или игнорируются. Время от времени будет проводиться проверка на фишинг. Результаты обычно неудивительны и неудовлетворительны. KnowBe4 сообщает, что около 38% неподготовленных сотрудников не проходят фишинговые тесты.

В целом, когда дело доходит до фишинга, обученные сотрудники хорошо умеют не вводить данные в формы. Они немного хуже нажимают на ссылки (35% отказов), но если есть вложение, показатели взлетают до 65%. Это число увеличивается до 90%, если письмо выглядит так, как будто оно пришло от узнаваемой внутренней учетной записи или псевдонима.

Если учесть, что эти вложения с большой вероятностью содержат вредоносное ПО, неудивительно, что средний сотрудник представляет наибольший риск для безопасности организации.

Почему не работают текущие модели обучения?

Хорошо обученные сотрудники работают лучше, чем необученные. Но, как показано выше, при изменении условий все еще существует значительный процент отказов. Почему обучение не работает лучше?

Традиционные методы обучения основаны на больших объемах памяти и нечастых, нечетких напоминаниях. Это не лучший способ добиться изменений или роста. Тренировка приносит пользу только в том случае, если она меняет поведение. Чтобы изменить поведение, материал необходимо запомнить и интегрировать в действия, которые становятся поведением по умолчанию. Традиционные методы ежегодного обучения не могут этого сделать. И мы знаем это уже более 135 лет.

Наука обучения

В 1885 году Герман Эббингаус изобразил результаты своих исследований памяти на графике и построил «кривую забывания». Его исследование показало, что частое вспоминание или повторное посещение тренировок снижает забвение. Старая школа не применяет эти знания, в результате чего 50% тренировок забываются в течение часа, что делает традиционные практики дорогими и непродуктивными.

Даже в 1970-х годах, примерно через сто лет после первого исследования Эббингауза, Джонстон и Персиваль сообщили, что у студентов было всего 10-18 минут «оптимального сосредоточения», прежде чем их внимание исчезло, унося с собой их способность удерживать информацию. И это было до появления смартфонов, которые еще больше уменьшили нашу концентрацию и объем внимания.

Наука показывает, что у людей есть только ограниченное окно в 10 минут или меньше, когда может происходить обучение. Если обучение проводится небольшими отрезками времени, удержание материала увеличивается на 90%.

Как геймификация может улучшить обучение?

Это весело - и наука также говорит нам, что все лучше учатся, когда им весело.

Текущие платформы и методы обучения для среднего сотрудника неинтересны, не сохраняются и не меняют поведения. Изменение обучения, включающее в себя геймификацию, вовлекает сотрудника в изучение материала, что улучшает обучение и способствует изменению поведения.

Обучение - это не часовая лекция, которую нужно проверять, это небольшие блоки целенаправленных инструкций, за которыми следует последовательный, но игривый просмотр информации. Это взаимодействие и постоянное воздействие укрепляют нейронные связи и паттерны, укрепляют позитивное поведение и новое обучение, а также создают комфорт и уверенность в новых навыках.

Почему это намного эффективнее?

Микрообучение наконец применяет науку об обучении и памяти. Он преобразует традиционную длинную форму обучения в небольшие, более короткие, чем единицы концентрации внимания, так что обучение может происходить. Затем он регулярно пересматривает информацию, чтобы оживить память и улучшить запоминание, что создает устойчивые навыки и изменение поведения.

Микрообучение и геймификация также более рентабельны, чем традиционные методы обучения. В течение часа часто забывают о длительных тренировках. Это обходится организациям в два раза - стоимости самого обучения и потерянного времени. Меньшее обучение лучше вписывается в расписание, является желанным «отвлечением» между сменами акцента и более эффективно с точки зрения обучения, удержания и затрат. Обучение превращается из «необходимости», отнимающей время, в «добираться», которое освежает разум и повышает безопасность организации.

Независимо от того, где находятся сотрудники, Интернет сегодня является частью бизнеса. Руководители службы безопасности знают, что часть обеспечения безопасности организации зависит от эффективности обучения сотрудников. Успешное обучение зависит от создания устойчивых изменений. Сотрудники должны регулярно помнить и проводить обучение. Наука уже более ста лет говорит нам, как улучшить обучение (и безопасность). Пришло время начать слушать». ***(Heather Stratford. A hundred-year-old secret is key to fighting cyberattacks // Security (https://www.securitymagazine.com/articles/94005-a-hundred-year-old-secret-is-key-to-fighting-cyberattacks). 15.01.2021).***

***

«В 16-м издании Доклада о глобальных рисках Всемирного экономического форума анализируются риски социальных расколов, проявляющиеся в постоянных и возникающих рисках для здоровья человека, росте безработицы, расширении цифрового разрыва, разочаровании молодежи и геополитической фрагментации. Среди самых высоких рисков воздействия на следующее десятилетие инфекционные заболевания занимают первое место, за ними следуют неудачи в борьбе с изменением климата и другие экологические риски; а также оружие массового уничтожения, кризисы средств к существованию, долговые кризисы и разрушение ИТ-инфраструктуры, отмечает Всемирный экономический форум.

В отчете также отмечается, что нарушение кибербезопасности является серьезной угрозой для мира. Всемирный экономический форум отмечает, что пандемия COVID-19 ускорила внедрение технологий, но выявила уязвимость и неподготовленность киберпространства и в то же время обострила технологическое неравенство внутри и между обществами.

Заглядывая в будущее, будет критически важно продолжать рассматривать кибербезопасность как стратегический бизнес-вопрос и развивать больше партнерских отношений между отраслями, бизнес-лидерами, регулирующими органами и политиками, поскольку эту проблему нельзя решать изолированно.

Хитеш Шет, президент и главный исполнительный директор Vectra, отмечает: «Без безопасных, высокофункциональных информационных технологий решение всех других кризисов, которые упоминаются в отчете, от климата до цифрового неравенства, становится намного сложнее. В течение многих лет наши хорошо понимаемые уязвимости в киберпространстве встречали слишком много риторики, слишком мало реальных действий. Я знаю политическую задачу формирования консенсуса для предотвращения чрезвычайной ситуации, которая еще не стала очевидной для всех. Тем не менее, атака на критическую инфраструктуру SolarWinds была вероятным предвестником грядущих событий. Крайне важно, чтобы мы срочно приняли меры по кибербезопасности как в государственном, так и в частном секторах».

Янив Бар-Даян, генеральный директор и соучредитель Vulcan Cyber, говорит: «Отказ кибербезопасности» правильно включен в четверку основных краткосрочных рисков и представляет собой явную и настоящую угрозу для мира. Еще более тревожным является прямая корреляция между кибербезопасностью и другими угрозами на глобальном горизонте рисков, такими как цифровое неравенство, поломки ИТ-инфраструктуры и даже террористические атаки и оружие массового уничтожения, поскольку традиционные определения как «терроризма», так и «оружия» становятся все более актуальными. больше связано с кибербезопасностью в нашем цифровом мире. К счастью, у нас больше контроля над рисками кибербезопасности, чем над другими угрозами, такими как инфекционные заболевания и экстремальные погодные явления. Тем не менее, отрасль ИТ-безопасности должна быть намного более внимательной и инициативной в улучшении кибергигиены нашей цифровой инфраструктуры». ***(World Economic Forum ranks cybersecurity failure as a significant global risk // BNP Media (https://www.securitymagazine.com/articles/94451-world-economic-forum-ranks-cybersecurity-failure-as-a-significant-global-risk). 27.01.2021).***

***

«В 2021 году компании планируют решать вопросы нехватки опытных специалистов и экономии бюджетов путём перевода функций IT и кибербезопасности на аутсорс.

Вот ещё некоторые тренды, которые видят эксперты:

В связи с массовым переходом на удалённый формат работы традиционной защиты периметра уже недостаточно, важно учитывать и домашние офисы. Необходимо использовать инструменты для сканирования уровня безопасности

рабочего пространства — от поиска уязвимостей в ПО до проверки на подключение к незащищённой точке Wi-Fi. Также потребуется более широкое распространение VPN, привилегированное управление доступом, системы мультифакторной аутентификации, внедрение более строгого мониторинга и обновление существующих планов по реагированию на киберинциденты;

Сервисные модели позволяют обеспечить требуемый уровень кибербезопасности с меньшим объёмом инвестиций. По данным «Лаборатории Касперского», 69% крупных компаний как в России, так и во всём мире планируют работать по MSP- или MSSP-модели. Это позволит им минимизировать вложения и перевести затраты из капитальных в операционные;

Тренинги для внутренних IT-специалистов должны включать обучение навыкам управления. В области кибербезопасности часто нужны очень узкие специалисты, поиск которых обходится бизнесу довольно дорого. В этом случае может помочь аутсорс. Однако компаниям, которые отдают на аутсорс ключевые компоненты кибербезопасности, следует развивать у внутренних команд навыки управления, чтобы они могли регулировать эти функции;

Растёт востребованность облачных сервисов и, соответственно, необходимость в их защите. Согласно опросу «Лаборатории Касперского», некорпоративное ПО и облачные сервисы, такие как социальные сети, мессенджеры или другие приложения, сотрудники используют для работы в подавляющем большинстве российских организаций (в 83% крупных и 87% небольших компаний). Чтобы обезопасить корпоративные данные, нужно более строго отслеживать то, как осуществляется доступ к облачным сервисам. Сотрудникам отделов по кибербезопасности следует отладить эти процессы и выработать навыки управления облачными средами и их защиты.

«Мы видим два новых важных тренда в том, что клиенты ожидают от корпоративной кибербезопасности. Во-первых, то, что защита должна быть качественной, перестало быть вопросом для обсуждения, а воспринимается как непреложный факт. Другой большой тренд — интеграция разных компонентов корпоративной безопасности от одного поставщика. Долгое время в индустрии было распространено мнение, что для обеспечения наиболее эффективной защиты лучше сочетать специализированные решения от разных вендоров. Теперь же организации стремятся к единому подходу и максимально возможной интеграции между разными технологиями безопасности», — говорит Александр Моисеев, директор по развитию бизнеса «Лаборатории Касперского». ***(«Лаборатория Касперского» рассказывает о трендах в корпоративной кибербезопасности на 2021 год // SecurityLab.ru (https://www.securitylab.ru/news/515967.php). 26.01.2021).***

***

«…Поскольку дистанционная работа в наши дни является характерным трендом почти каждого сектора экономики, обеспечивающие её технологии стали важнейшим краеугольным камнем для бизнеса. Попробуем рассмотреть, как к реалиям распределённой рабочей силы адаптируются технологии кибербезопасности.

Прогнозы безопасности. Технологии

Организациям с ограниченными ресурсами и бюджетом кибербезопасности надоело покупать монолитные SIEM-решения с сомнительной окупаемостью инвестиций, довольствуясь невнятными обещаниями их полезности в будущем. Технологические покупки следует ориентировать на результат: решения по управлению безопасностью в целом и SIEM, в частности, должны оправдывать потраченные на них средства. Необходимо, чтобы каждый вложенный доллар можно было наглядно связать с полученными ценными сведениями, имеющими решающее значение для обеспечения безопасности организации.

Автоматизация – сейчас настало самое время, чтобы изменить наше отношение к ней. Ран Тамир (Ran Tamir), вице-президент по продукции фирмы Pcysys, отмечает, что без расширения использования автоматизации невозможно наладить непрерывное и точное тестирование, жизненно важное для поддержания и улучшения состояния кибербезопасности организации.

Более удобная аналитика с улучшенным соотношением между сигналами о реальных угрозах и ложными срабатываниями, это то, что в 2021 году клиенты будут всё чаще требовать от своих провайдеров SIEM. «Аналитика должна стать более простой в поддержке и настройке, обеспечивать высокую степень точности и объяснимости результатов с минимальным вмешательством человека», – говорит Дерек Лин (Derek Lin), главный специалист по данным в Exabeam. По его словам, прогностическая аналитика, подкрепленная надлежащими инженерными знаниями и опытом в области безопасности, выведет UEBA на новый уровень сложности, эффективности и полноты.

Консолидацию отрасли предсказывает Грант Леонард (Grant Leonard), соучредитель Castra Managed Services. Он считает, что в сегменте SIEM останется место всего для нескольких крупнейших игроков, а онпремисные SIEM-решения практически исчезнут в течение следующих десяти лет. Новый год будет отмечен началом консолидации провайдеров управляемых сервисов безопасности (MSSP) и обнаружения и реагирования (MDR): мелкие и крупные, но негибкие, игроки сойдут со сцены, уступив место тем, кто использует инструменты ML/SOAR, а также XDR (межуровневое обнаружение и реагирование). Наконец, на фоне этой консолидации рынка, будет продолжать расти значение оркестровки и автоматизации для MSSP/MDR, которые, однако, в большинстве случаев не смогут полностью оправдать возлагаемых на них надежд.

Резкое увеличение количества атак на API-интерфейсы, использующих их уязвимости и ошибки конфигурирования, ожидает Колин Андерсон (Colin Anderson) из Levi Strauss. С широким распространением облачных приложений, работающих с такими API, это еще один вектор атаки, демонстрирующий настоятельную потребность в решении данной проблемы безопасности в будущем.

Рекомендации

Основываясь на своих прогнозах, команда Exabeam выработала несколько рекомендаций для специалистов по безопасности, составляющих планы на 2021 год.

• Для того, чтобы успешно противостоять всё более частым атакам, связанным с учётными данными, организациям из разных отраслей рекомендуется инвестировать в поведенческую аналитику пользователей и сущностей (UEBA). В

сочетании с машинным обучением это позволит гарантировать, что вредоносная активность не останется незамеченной. Кроме того, возможность выявлять аномальное поведение законных пользовательских аккаунтов позволит аналитикам отделов безопасности (SOC) распознавать как просто скомпрометированных пользователей, так и злонамеренных инсайдеров.

• Выявление недочётов и осуществление инициатив модернизации инфраструктуры должны подкрепляться интеллектуальным анализом вашей сети и приложений. Мало отслеживать только конкретные риски – убедитесь, что ваши решения являются комплексными и способны обнаруживать активность, отклоняющуюся от нормальной (это также поможет предотвратить усталость от предупреждений).

• Расширение полномочий групп SOC будет иметь решающее значение для улучшения ваших программ и процессов безопасности. Налаживайте контакты между CISO и их группами безопасности (аналитиками и т. д.), чтобы обеспечить действующий канал связи с исполнительной командой. Для того, чтобы управленческие решения могли приниматься быстро и эффективно, директора по информационной безопасности должны обращаться к совету директоров, генеральному директору, ИТ-директору или финдиректору, имея наготове все нужные данные и обоснования.

• В ещё одной рекомендации по процессам Exabeam предлагает сосредоточиться на обучении основам и передовым практикам безопасности сотрудников, подрядчиков и даже привлекаемых посторонних лиц – всех, кто получает удалённый доступ к приложениям и данным организации за пределами её брандмауэров. Это позволит снизить опасность киберугроз и риски утечки данных.

• Тесты, тесты, тесты. Только тестирование способно обеспечить отделам безопасности понимание истинного состояния киберзащиты их сетей. Никакие готовые решения или их комбинации не сделают вас полностью защищёнными. Без понимания границ возможностей ваших инструментов, растущая поверхность всё более изощренных атак ввергнет вас в огромный и неопределенный риск. Лучшее, что вы можете сделать, – это вновь и вновь тестировать, чтобы определить приоритетные элементы управления, которые необходимы для укрепления безопасности сегодняшней уникальной среды распредёленной рабочей силы.

• И наконец, при выборе инструментов и решений безопасности руководствуйтесь не только экономической выгодой и окупаемостью. Они должны органично взаимодействовать с остальной частью вашего стека безопасности и ИТ и снижать операционную нагрузку на вашу команду SOC.

Заключение

Для лучшего противодействия киберпреступникам, пытающимся воспользоваться возможностями, предоставленными продолжающейся в 2021 г. тенденцией перехода на удалённую модель работы, руководителям отделов ИТ и безопасности необходимо тщательно изучить аспекты взаимодействия их людей, процессов и технологий. Это поможет организациям эффективно конкурировать в этой непредсказуемой среде, обезопасить своих сотрудников и клиентов и оптимизировать отделы безопасности». ***(Максим Юстус. 10 прогнозов кибербезопасности на 2021 г. Технологии // Компьютерное Обозрение***

(https://ko.com.ua/10_prognozov_kiberbezopasnosti_na_2021_g_tehnologii_136041). 22.01.2021).

***

Сполучені Штати Америки

«Команда Байдена-Харриса объявила 8 января еще о 21 кандидате в Совет национальной безопасности (СНБ) новой администрации, в том числе двое, которые наверняка будут играть важную роль в политике кибербезопасности.

Команда по переходу назначила Таруна Чабру на должность старшего директора по технологиям и национальной безопасности и Кейтлин Дуркович на должность старшего директора по устойчивости и реагированию.

И Чабра, и Дуркович пришли в Совет национальной безопасности с опытом работы в администрации Обамы-Байдена, а также в сфере аналитических центров. Теперь каждый из них будет играть ключевую роль в консультировании новой администрации по вопросам национальной безопасности и внешней политики…

Чабра возвращается в СНБ после того, как сначала работал директором по стратегическому планированию и директором по правам человека и вопросам национальной безопасности в СНБ администрации Обамы. Чабра также работал в Пентагоне спичрайтером министра обороны. Чхабра перейдет на эту должность из Джорджтаунского университета, где он работает старшим научным сотрудником Центра безопасности и новых технологий. Ранее он стажировался в Брукингском институте и Пенсильванском университете.

Дуркович пришел в NSC из аналитического центра Атлантического совета и в настоящее время работает в переходной группе в составе группы проверки Министерства внутренней безопасности (DHS). Она работала в DHS при администрации Обамы-Байдена в качестве начальника штаба Управления национальной защиты и программ, которое предшествовало Агентству по кибербезопасности и безопасности инфраструктуры в DHS». ***(LAMAR JOHNSON. Biden-Harris Administration Adding Two More Cybersecurity Experts to NSC // MeriTalk (https://www.meritalk.com/articles/biden-harris-administration-adding-two-more-cybersecurity-experts-to-nsc/). 08.01.2021).***

***

«Управление генерального инспектора (OIG) Министерства торговли объявило в прошлом месяце, что будет проводить анализ возможностей Департамента по обмену данными о киберугрозах в соответствии с Законом о совместном использовании информации о кибербезопасности от 2015 года, который создает структуры для обмена данными об угрозах с правительством и предприятиями частного сектора.

Основное внимание в отчете будет уделяться тому, является ли текущая политика обмена данными достаточной, если «индикаторы киберугроз и защитные

меры должным образом классифицированы», и делится ли правительство индикаторами угроз и стратегиями защиты.

«Мы поможем составить межведомственный отчет о действиях, предпринятых исполнительной ветвью федерального правительства для выполнения этого звания в течение календарных 2019–2020 годов», - говорится в меморандуме. «Мы планируем немедленно приступить к этой работе».

Результат обзора OIG по торговле будет включен в обширный отчет о более широкой деятельности правительства по обмену данными о киберугрозах, который будет охватывать период 2019-2020 годов и будет выпущен OIG разведывательного сообщества в декабре 2021 года.

Другие агентства, участвующие в окончательном отчете, будут включать министерства обороны, энергетики, внутренней безопасности, юстиции и казначейства, а также Управление директора национальной разведки.

Закон 2015 года предусматривал беспрепятственный обмен данными об угрозах кибератак, но с момента его принятия поступил ряд жалоб на скорость и эффективность процесса обмена данными.

Улучшение возможностей совместного использования кибер - угроз является целью, что лишь немногие из них не согласились с, но только становится более важным процесс в свете когда-либо более сложных атак, таких как продолжение выпадений из SolarWinds взламывать российскими государственными структурами.

«Угрозы кибербезопасности… требуют уникального уровня сотрудничества между государственным и частным секторами», - написал 17 декабря президент Microsoft Брэд Смит в своем блоге, который иллюстрирует ценность обмена разведданными.

«Современная технологическая инфраструктура, от центров обработки данных до оптоволоконных кабелей, чаще всего принадлежит и управляется частными компаниями», - сказал Смит. «Они представляют собой не только большую часть инфраструктуры, которую необходимо защитить, но и поверхность, на которой обычно впервые обнаруживаются новые кибератаки. По этой причине для эффективной киберзащиты требуется не просто коалиция мировых демократий, но и коалиция с ведущими технологическими компаниями». ***(LAMAR JOHNSON. Commerce OIG Sets Review of Cyber Threat Data Sharing Capabilities // MeriTalk (https://www.meritalk.com/articles/commerce-oig-sets-review-of-cyber-threat-data-sharing-capabilities/). 08.01.2021).***

***

«Белый дом выпустил Национальный план морской кибербезопасности - план для Министерства внутренней безопасности (DHS) по разработке и развертыванию кадров морской кибербезопасности для мониторинга, защиты и смягчения киберугроз для морского сектора.

Согласно плану, опубликованному Белым домом в декабре 2020 года, DHS через береговую охрану «разработает карьерные возможности в области кибербезопасности, стимулы, требования к непрерывному образованию и стимулы для удержания кадров для создания компетентных морских кибер кадров». DHS

также будет координировать свои действия с «другими соответствующими департаментами и агентствами».

Сообщается, что «Федеральные силы кибербезопасности на море существуют, но не имеют достаточного персонала, ресурсов и обучения для мониторинга, защиты и смягчения киберугроз в морском секторе». Новый план направлен на восполнение существующих пробелов и «обеспечение максимальной защиты критически важной морской инфраструктуры».

DHS, работая с ВМС США, также будет сотрудничать с частным сектором в целях «повышения квалификации в области кибербезопасности на море». Военно-морской флот и береговая охрана сосредоточат свое внимание на исследованиях и применении кибербезопасности портов и судов, а также на обменах персоналом с промышленными предприятиями и национальными лабораториями.

Береговая охрана будет следить за развитием и развертыванием кадровых ресурсов морской кибербезопасности. Береговая охрана направит группы киберзащиты «для поддержки координации федеральной морской безопасности на объектах, регулируемых MTSA [Закон о безопасности морского транспорта], и помощи в морских расследованиях, если потребуется».

В отчете Белого дома также подчеркивается важность «внедрения стандартов морской кибербезопасности, обмена передовым опытом и защиты морской территории, которая питает нашу экономику и защищает нашу национальную безопасность». ***(GRACE DILLE. White House Issues Plan to Strengthen Maritime Cybersecurity Workforce // MeriTalk (https://www.meritalk.com/articles/white-house-issues-plan-to-strengthen-maritime-cybersecurity-workforce/). 05.01.2021).***

***

«Когда 6 января враждебные актеры проникли в здание Капитолия, они получили доступ к отдельным комнатам и офисам и оставались на свободе в пределах комплекса Капитолия более двух часов.

У нас есть сообщения о краже вещей. Один отчет поступил от исполняющего обязанности прокурора округа Колумбия Майкла Шервина, который заявил, что «предметы, электронные предметы были украдены из офисов сенаторов, документы и ... мы должны определить, что было сделано для смягчения этого». Мой местный сенатор Джефф Меркли (демократ) сообщил, что по крайней мере один ноутбук был украден.

На устранение последствий этой атаки для кибербезопасности уйдут месяцы, учитывая украденные ноутбуки, потерянные данные и потенциальный шпионаж. Вот взгляните на проблемы кибербезопасности.

ПРОБЛЕМЫ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Хотя наблюдение, несомненно, отслеживало многие из сотен человек, проникших внутрь здания, мы не можем предположить, что знаем точные посекундные передвижения каждого, кто вошел внутрь. Это означает, что неизвестно, какие меры были приняты против цифрового оборудования внутри здания.

Пароли, документы, коды доступа, а также конфиденциальная или секретная информация могли быть украдены. Мы также должны предположить, что

некоторые компьютеры могли быть скомпрометированы, на них было загружено вредоносное ПО. Поскольку вредоносное ПО является ключом к любому системному проникновению, мы должны предположить, что злоумышленники получили постоянный, скрытый, постоянный доступ к системам здания Капитолия.

По всей вероятности, только небольшое количество машин было взломано. Но учитывая конфиденциальный характер информации, хранящейся на цифровом оборудовании внутри Капитолия, и учитывая, что невозможно быстро установить, какие устройства были взломаны, федеральный ИТ-персонал должен предположить, что ВСЕ цифровые устройства в Капитолии были скомпрометированы.

Ситуация на самом деле хуже, чем может показаться на первый взгляд. Согласно хронологии USA Today, Конгресс снова собрался в 8 часов вечера 6 января. Вероятно, что штатные компьютеры начали использовать компьютеры всего через несколько минут после возобновления работы Конгресса. Очевидно, что не было возможности полностью поднять и мгновенно заменить тысячи машин. Таким образом, с того момента и до настоящего времени члены и их сотрудники использовали цифровые устройства, которые могли быть взломаны. Это означает, что все коммуникации, файлы и сетевые соединения с этими устройствами также могли быть скомпрометированы.

ФИЗИЧЕСКИЙ ДОСТУП ПОВЫШАЕТ СТАВКИ

Если бы компьютеры Капитолия подверглись атаке с помощью традиционного взлома, основанного на вредоносном ПО, а затем взломали Интернет, смягчение последствий могло бы быть умеренно простым, если не неудобным и болезненным. Системы могли быть просканированы на наличие вредоносных программ и - в наиболее важных случаях - жесткие диски могли быть обнулены или заменены.

Но в здании находились сотни посторонних людей, людей, которых сфотографировали, получив доступ к столам и личным кабинетам членов. Эти люди могли пойти куда угодно в здании.

Мы также должны предположить, что какие-то иностранные актеры вошли в здание, смешавшись с толпой. Да, я знаю, это звучит параноидально, но выслушайте меня. Мы знаем, что Россия и другие страны уже некоторое время проводят кибератаки против Америки.

Мы также знаем, что окончательное заверение Конгрессом бюллетеней для президентских выборов 2020 года было конституционно назначено на 6 января - и из-за горячей риторики почти наверняка возникли толпы и беспорядки.

Поэтому весьма вероятно, что вражеские (или заклятые) актеры также знали о возможности беспорядков вокруг здания Капитолия. Хотя конкретные детали того, что именно будет разворачиваться 6 января, было невозможно предсказать, есть все основания ожидать, что международные обработчики сочтут разумным держать небольшие группы агентов в режиме ожидания. Таким образом, если представится возможность, они могут тайком вставить этих агентов в ситуацию.

Следовательно, мы должны предположить, что некоторые из людей, проникших на Капитолийский холм, вероятно, были иностранными актерами. И исходя из этого наблюдения, мы должны ожидать, что один или несколько из тех

иностранных игроков, которые проникли внутрь, предприняли какие-то физические действия против машин, которые обычно находятся вне досягаемости.

ФИЗИЧЕСКИЙ ДОСТУП - ЭТО БОЛЬШЕ, ЧЕМ ПРОСТО КРАЖА КОМПЬЮТЕРОВ

Когда вражеский агент получает физический доступ, многое может случиться. И под большим количеством я имею в виду скрытые атаки, которые потребуют от ИТ-специалистов Капитолия усилий по восстановлению выжженной Земли. Во-первых, давайте осознаем, что вредоносные программы часто не проявляют себя, пока не произойдет установленный период времени или триггер. Так что машины, которые кажутся совершенно нормальными, вполне могут быть троянскими конями.

Возможно, машины были открыты, а флеш-накопители или даже дополнительные диски были помещены внутрь машин, которые затем были снова запломбированы. С помощью отвертки можно открыть оболочку ПК в корпусе Tower, вставить USB-накопитель в открытый внутренний порт и снова запечатать его через минуту или две. Они могут никогда не быть обнаружены.

Когда Stuxnet дестабилизировано на центрифугах в Натанзе в Иране, червь был доставлен через USB - накопителей контрабандных на объект. Что касается службы безопасности Капитолия, то в здании Капитолия находились сотни людей. Эффективной атакой было бы просто оставить случайные универсальные USB-накопители в разных ящиках и на разных столах. Несомненно, кто-нибудь увидит диск, решит, что это его собственный, и подключит его. Вредоносное ПО доставлено.

Возможны и другие физические атаки. Ранее мы говорили о зарядном устройстве USB с беспроводным кейлоггером. Мы писали о Power Pwn, устройстве, которое выглядит как удлинитель, но скрывает инструменты взлома беспроводной сети. Мы обсуждали, как против офисов в ЕС была запущена атака типа «злоумышленник посередине», перекачивающая трафик Wi-Fi нелегальному слушателю.

С сотнями людей внутри Капитолия подобные устройства можно было оставить на месте. На их обнаружение могут уйти недели или месяцы, особенно если они были оставлены как беспорядок, чтобы их использовали случайные сотрудники, когда им понадобится запасное оборудование.

ЧТО НАДО ДЕЛАТЬ

Есть некоторые передовые методы ИТ, которые могут снизить риск. Сеть микро-сегментация может предотвратить вредоносную от скрещивания между зонами, например. Но никакие методы сетевой безопасности не могут полностью предотвратить физическую атаку.

Здание Капитолия необходимо полностью очистить. Все машины должны быть просканированы. Любой настольный ПК, который не герметичен, необходимо открыть и тщательно осмотреть его внутренние компоненты. Слоты для USB-накопителей должны быть заблокированы, чтобы сотрудники Capitol Hill не могли подключать случайные USB-накопители. Необходимо многократно сканировать здание по комнате, этаж за этажом на предмет передачи лучистого сигнала.

Сотрудники Конгресса должны быть осведомлены о том, на что обращать внимание, о передовых методах работы и о том, как проявлять особую осторожность, даже если это требует дополнительного времени.

Каждое цифровое устройство на территории Капитолия должно считаться подозрительным. Важно поддерживать высокий уровень безопасности даже после того, как активные машины были протестированы и просканированы, потому что нам нужно следить за отложенными угрозами и атаками, которые скрываются, ожидая их возможности инициировать доступ.

НАРУШЕНИЯ ЗАКОНА О ШПИОНАЖЕ

Наконец, все, кто участвовал в нападении, особенно те, кто проник в здание, должны быть привлечены к ответственности по всей строгости закона и, возможно, даже обвинены в нарушениях Закона о шпионаже. Хотя некоторых участников можно было охарактеризовать как «патриотов» или разгневанных «хороших людей», факт остается фактом: их действия могли послужить прикрытием для актов шпионажа со стороны врагов нашей страны.

Я слышу, что ты говоришь. «Но Дэвид, разве это не немного паранойя, когда думаешь, что другие страны воспользуются нашими собственными внутренними спорами?» В порядке отлично. Никто бы этого не сказал. Вместо этого было бы много размахивать кулаками и кричать на меня. Но для наших целей перейдем к гражданской версии.

И нет, это не параноя. Россия вмешалась в выборы 2016 года. Это часть базового ремесленного мастерства - разжигать гнев и разногласия среди населения цели. Мы знаем, что вмешательство России привело к гневу, который мы все испытываем, хотя наши собственные политики определенно использовали это в своих эгоистических интересах.

Атака на здание Капитолия была полностью основана на гневе. Учитывая, что сеяние беспорядков является важной частью сценария действий России, вполне вероятно, что они хорошо осознавали значение даты 6 января и были вполне готовы извлечь из этого выгоду в полной мере. И все это приводит нас к шпионажу, осуществляемому иностранными акторами, но, скорее всего, при поддержке и подстрекательстве одураченных или замешанных в ярости американцев.

Те, кто штурмовали Капитолийский холм, возможно, нарушили 18 § 792 Кодекса США - Укрывательство или сокрытие людей. Этот кодекс прост и гласит: «Тот, кто укрывает или скрывает любого человека, которого он знает или имеет разумные основания полагать или подозревать, совершил или собирается совершить преступление». Если можно доказать, что кто-либо из злоумышленников может просто подозревать, что внешний агент проникнет в здание вместе с ними, они нарушают этот статут.

Они также могли нарушить 18 § 793 Кодекса США - Сбор, передача или потеря информации защиты. Это один из самых важных вопросов, открывающийся с "Кто бы то ни было, с целью получения информации, касающейся национальной обороны, с намерением или основанием полагать, что эта информация должна быть использована во вред Соединенным Штатам или в пользу какой-либо иностранная нация ... "Остановка или отмена выборов определенно можно рассматривать" в

ущерб Соединенным Штатам ", и, опять же, если какая-либо из этих сведений раскрывается иностранной державе - даже через фото в Твиттере, это серьезное нарушение.

Далее перечисляется широкий спектр государственных ресурсов, которые в случае взлома могут быть нарушены, включая»... здание, офис, исследовательскую лабораторию или станцию или другое место, связанное с национальной обороной, находящееся в собственности или построенное или находящееся в процессе строительство осуществляется Соединенными Штатами или под контролем Соединенных Штатов, или любого из их офицеров, департаментов или агентств... "Ясно, что здание Капитолия подпадает под это, тем более что комитеты Конгресса действительно имеют дело с строго секретной информацией.

Люди, совершающие преступления в соответствии с этими кодексами, «будут наказаны штрафом по этой статье или лишением свободы на срок не более десяти лет, либо и того, и другого».

Именно с 18 Кодексом США § 794 - Сбор или передача оборонной информации в помощь иностранным правительствам, дела начинают становиться серьезными. Закон начинается со слов «Кто бы то ни было с намерением или основанием полагать, что он должен быть использован во вред Соединенным Штатам или в пользу иностранного государства», и, опять же, блокирование санкционированного Конституцией удостоверения выборов является вредно для Соединенных Штатов.

Но вот где это становится рискованным для тех, кто вторгся 6 января. Устав продолжает:

... передает, доставляет или передает, или пытается передать, доставлять или передавать любому иностранному правительству, любой фракции, партии, вооруженным силам или военно-морским силам в иностранной стране, признанной или непризнанной Соединенными Штатами, или любому их представителю, должностному лицу, агенту, сотруднику, субъекту или гражданину, прямо или косвенно, любой документ, письменность, кодовая книга, сигнальная книга, эскиз, фотография, фотографический негатив, чертеж, план, карта, модель, заметка, инструмент, приспособление или информация, относящаяся к национальной обороне ...

Этот закон очень широкий и по сути гласит, что даже если доставка осуществляется кому-то, официально не признанному иностранным гражданином, или даже если доставка осуществляется косвенно (например, через друга, аукцион eBay, фотографии в Instagram и т. нарушение. Так мы видели картинки столов с документами, экранов с электронной почтой и т. Д.? Если какой-либо элемент на любом из этих изображений был конфиденциальным или засекреченным и мог быть увиден внешним агентом, срабатывает этот пункт.

Наказание? Что ж, пусть статут говорит сам за себя: «наказывается смертью или лишением свободы на любой срок или пожизненно». Ой!

Давайте проясним здесь. Большинство нападавших были американцами. И какими бы подлыми ни были их действия - а вторжение в конституционную практику и ее прерывание - презренно, независимо от того, на какой стороне

прохода вы находитесь - большинство из них, скорее всего, думали, что действуют от имени США, а не намерение повредить его.

Закон часто учитывает умысел. Но когда дело доходит до шпионажа, у закона очень большой молоток. Соединенные Штаты не любят шпионаж. С тысячами людей в толпе за пределами здания и сотнями, которые ворвались внутрь, у тех, кто совершал преступление, не было возможности узнать, кем могли быть их товарищи по мафии в то время. Обеспечение прикрытия для вражеских агентов, даже если можно утверждать, что это было сделано по наивности или глупости, по-прежнему обеспечивает прикрытие для вражеских агентов.

Это будет длиться месяцами или годами как в наших судах, так и в разведывательном сообществе Соединенных Штатов. Если какая-либо защищенная информация, полученная в результате этого взлома, попадет в чьи-либо иностранные руки, ставки неизмеримо возрастут, и эти старые добрые мальчики из средней Америки в отцовских джинсах и бейсболках или козьих рогах, краске для лица и меховых бикини вполне могут оказаться подверженные всей мощи и гневу правительства Соединенных Штатов - того самого правительства, которое они пытались свергнуть.

ВЫ МОЖЕТЕ ПОМОЧЬ

InfraGard опубликовал недавнее предупреждение, которым я сейчас с вами делюсь. Полевой офис Федерального бюро расследований в Вашингтоне обращается за помощью к общественности в выявлении лиц, незаконно проникших в здание Капитолия США 6 января 2021 года в Вашингтоне, округ Колумбия.

Кроме того, ФБР предлагает вознаграждение в размере до 50 000 долларов за информацию, ведущую к местонахождению, аресту и осуждению лиц, ответственных за установку самодельных бомб в Вашингтоне 6 января 2021 года.

Примерно в 13:00 по восточному стандартному времени 6 января 2021 года несколько правоохранительных органов получили сообщения о предполагаемой самодельной бомбе с проводами в штаб-квартире Республиканского национального комитета (RNC), расположенной по адресу: 310 First Street Southeast в Вашингтоне, округ Колумбия.

Примерно в 13:15 по восточному стандартному времени в штаб-квартире Национального комитета Демократической партии (DNC) по адресу 430 South Capitol Street Southeast # 3 в Вашингтоне, округ Колумбия, было сообщено о второй подозреваемой самодельной бомбе с аналогичными дескрипторами.

Любого, у кого есть информация об этих лицах, или любого, кто был свидетелем каких-либо незаконных насильственных действий в Капитолии или поблизости от него, просят позвонить по бесплатному телефону ФБР по телефону 1-800-CALL-FBI (1-800-225-5324). устно сообщить подсказки. Вы также можете отправить любую информацию, фотографии или видео, которые могут иметь отношение к делу, на сайте fbi.gov/USCapitol. Вы также можете связаться с вашим местным офисом ФБР или ближайшим американским посольством или консульством». ***(David Gewirtz. Capitol attack's cybersecurity fallout: Stolen laptops, lost data and possible espionage // ZDNet (https://www.zdnet.com/article/capitol-attacks-cybersecurity-fallout-stolen-laptops-lost-data-and-possible-espionage/). 11.01.2021).***

***

«5 января 2020 года закон HR 7898 стал законом о внесении поправок в Закон о медицинских информационных технологиях для экономического и клинического здравоохранения (Закон HITECH), 42 USC 17931, чтобы потребовать, чтобы «признанные методы кибербезопасности» учитывались министром здравоохранения и социальных служб (HHS) при определении любых штрафов в соответствии с Законом о переносимости и подотчетности медицинского страхования (HIPAA), результатов аудита или средств смягчения последствий. Новый закон предоставляет серьезный стимул для охваченных страхованием организаций и деловых партнеров применять «признанные методы кибербезопасности» и схемы снижения рисков при соблюдении стандартов конфиденциальности и безопасности HIPAA для снижения риска, связанного с угрозами безопасности и определениями соблюдения требований HHS. В частности, более раннее принятие установленной, формализованной и признанной структуры кибербезопасности может значительно защитить организации от нормативного правоприменения после последующих инцидентов безопасности или утечки данных.

Поправка требует, чтобы при принятии решений, касающихся штрафов, сокращения продолжительности и объема проверок или согласования мер по смягчению последствий, секретарь должен учитывать, «продемонстрировала ли организация надлежащим образом, что она не менее чем за предыдущие 12 месяцев признала действующие методы безопасности, которые могут»:

(1) смягчить наложение штрафов в соответствии с разделом 13410 Закона о HITECH;

(2) привести к досрочному и благоприятному прекращению аудита в соответствии с 13411 Закона о HITECH; или же

(3) смягчить меры, которые в противном случае были бы согласованы в любом соглашении относительно устранения возможных нарушений правила безопасности HIPAA между покрываемым юридическим лицом или деловым партнером и HHS.

Термин «признанные методы обеспечения безопасности» означает «стандарты, руководящие принципы, передовой опыт, методологии, процедуры и процессы, разработанные в соответствии с разделом 2 (c) (15) Закона о Национальном институте стандартов и технологий (NIST), подходы, провозглашенные в соответствии с раздел 405 (d) Закона о кибербезопасности 2015 года, а также другие программы и процессы, касающиеся кибербезопасности, которые разработаны, признаны или обнародованы в соответствии с нормативными актами других законодательных органов. Такая практика должна определяться юридическим лицом или деловым партнером в соответствии с Правилом безопасности HIPAA». В соответствии с Правилом безопасности HIPAA, это широкое определение предоставляет защищенным организациям и деловым партнерам гибкость для внедрения разумных и надлежащих «признанных практик безопасности» в соответствии с размером, масштабы и сложность их организаций. Рекомендуемыми отправными точками для определения признанных практик

безопасности было бы использованиеСпециальная публикация NIST 800-66 ред. 1 и Практики кибербезопасности в сфере здравоохранения (Управление угрозами и защита пациентов).

В свете защитного воздействия этого нового закона организациям, которые еще не внедрили «признанные методы обеспечения безопасности», следует подумать о том, чтобы сделать это сейчас. Первым важным шагом к выбору разумных и подходящих методов обеспечения безопасности является проведение основанных на оценке рисков оценок вероятных угроз безопасности, субъектов угроз и уязвимостей. На основе результатов такой оценки организации могут затем определить возможные противодействующие общепризнанным методам обеспечения безопасности, которые могут снизить риск инцидента безопасности или утечки данных, возникающих в первую очередь, и снизить риск последующего применения нормативных требований. В соответствии с новой поправкой к Закону о HITECH, принятие признанных методов обеспечения безопасности может положительно повлиять на определение уровня штрафов и других принудительных мер в случае более поздней утечки данных или другого нарушения». ***(Brian G. Cesaratto, Patricia Wagner, Alaap Shah. HITECH Act Amendment Incentivizes Adoption of NIST and Other Recognized Cybersecurity Safeguards as a Defense or Mitigation to HIPAA Enforcement // Epstein Becker & Green, P.C. (https://www.healthlawadvisor.com/2021/01/08/hitech-act-amendment-incentivizes-adoption-of-nist-and-other-recognized-cybersecurity-safeguards-as-a-defense-or-mitigation-to-hipaa-enforcement/). 08.01.2021).***

***

«Избранный президент Джо Байден и избранный вице-президент Камала Харрис вступят в должность 20 января 2021 года, открывая новый набор нормативных и законодательных приоритетов в течение следующих четырех лет. Главным из приоритетов администрации Байдена будет реагирование на пандемию коронавируса, что может включать в себя пакет инфраструктуры для стимулирования экономики, и это созрело для включения реформ, связанных с кибербезопасностью. Однако принятие закона на 117-м Конгрессе, в котором демократы, вероятно, будут иметь незначительное большинство в Палате представителей и Сенате, потребует поддержки обеих партий.

Кибербезопасность традиционно является двухпартийным вопросом и может быть одной из таких областей, где законодатели и администрация Байдена могут найти общий язык, особенно в вопросах, касающихся транспорта и инфраструктуры. Конфиденциальность, напротив, была более частым вопросом в последние несколько лет, но продолжающиеся переговоры Конгресса по всестороннему законопроекту о конфиденциальности также могут повлиять на транспортную отрасль. Отдельно новая администрация, вероятно, будет использовать регуляторные реформы и правоприменение для повышения кибербезопасности и защиты конфиденциальности. Ниже приведены некоторые реформы и усилия, связанные с кибербезопасностью и конфиденциальностью, которые могут быть предприняты при администрации Байдена.

Расширение 5G

Платформа кампании избранного президента Байдена включала развертывание мобильных сетей пятого поколения (5G), чтобы обеспечить более быструю и надежную связь, но вместе с этим возрастают киберугрозы и риски для транспортного сектора. Таким образом, законодательство может включать новые требования к поставщикам и стандарты для разработчиков оборудования и программного обеспечения, чтобы хакеры не могли использовать существующие или новые уязвимости безопасности. Комиссия по киберпространству по солярию (CSC), выпустившая 82 рекомендации в своем отчете за март 2020 года «Предупреждение с завтрашнего дня», "ориентирован на безопасность 5G и, вероятно, продолжит продвигать законодательство в 2021 году, направленное на решение этих проблем. Из этих рекомендаций 26 стали законом в соответствии с Законом о государственной обороне на 2021 финансовый год (NDAA), что указывает на то, что рекомендации отчета поддерживаются республиканцами и демократами. Некоторые из оставшихся и соответствующих положений можно было бы включить в пакет инфраструктуры стимулирования, аналогичный Закону о восстановлении и реинвестировании Америки 2009 года, который тогдашний вице-президент Байден помогал администрации Обамы в переговорах по устранению последствий Великой рецессии.

Обозначение критической инфраструктуры

Также в пакете инфраструктуры Конгресс может стремиться установить стандарты корпоративной ответственности и процесс реагирования на атаки, которые происходят на критически важной инфраструктуре, такой как транспорт, а также стандарты для устранения или снижения киберрисков. Такое положение может предусматривать новые требования к аудиту и уведомлению для транспортного сектора при возникновении инцидента безопасности. Примечательно, что защита критически важной инфраструктуры - краеугольный камень отчета CSC - будет приоритетом для администрации Байдена с учетом недавно получившей широкую огласку и масштабных кибератаках федеральных правительственных агентствах подозреваемыми российскими хакерами. Атака подчеркивает существующие опасения относительно рисков, связанных с консолидацией ключевых поставщиков программного обеспечения для корпоративной Америки и федерального правительства, а иногда и того и другого, так что одна уязвимость может вызвать волновой эффект, превышающий исторически возможный.

Государственно-частное партнерство

Ожидайте, что администрация Байдена и Конгресс сосредоточатся на создании государственно-частных партнерств для координации кибер-проблем. С административной точки зрения это может включать расширение полномочий Агентства по кибербезопасности и безопасности инфраструктуры (CISA), а также увеличение ресурсов и охвата частного сектора. Например, в недавней кибератаке на федеральные агентства CISA взяла на себя ведущую роль в выпуске предупреждений и директив., и в координации с частным сектором. Администрация Байдена, вероятно, будет отражать подход администрации Обамы, особенно в том, что касается более активного участия в кибербезопасности для обеспечения высокого уровня координации. Законодательно это может включать

новые программы, которые стимулируют государственно-частное сотрудничество и включают безопасные гавани для частного сектора в обмен на координацию с правительством.

Новый национальный кибердиректор

В соответствии с недавно принятым NDAA на 2021 финансовый год в Исполнительном аппарате президента будет учрежден национальный кибердиректор. Эта реформа была первоначально рекомендована в отчете CSC. Учитывая недавнюю кибератаку на федеральные агентства, роль кибердиректора чрезвычайно важна. Директор будет выполнять функции главного советника президента по вопросам кибербезопасности, а также вести координацию стратегии и политики кибербезопасности на национальном уровне в рамках правительства и частного сектора. Директор может повлиять на транспортную отрасль с точки зрения киберответа и координации, в зависимости от человека, который занимает должность, и роли, которую он берут на себя в координации с федеральным, государственным, местным, племенным и территориальным правительством и частным сектором.

Руководство по кибербезопасности транспортных средств

В настоящее время Национальное управление безопасности дорожного движения (НАБДД) Министерства транспорта США работает над обновлением руководства по кибербезопасности для транспортных средств «Лучшие практики кибербезопасности для безопасности современных транспортных средств». Руководство в настоящее время рассматривается в Белом доме Управления и (АБУ) Бюро бюджета информационных и по вопросам регулирования (ОИР). По завершении межведомственной проверки НАБДД запросит общественное обсуждение, и запрос будет опубликован в Федеральном реестре. Заинтересованные стороны, заинтересованные в транспортном секторе, и особенно производители оригинального оборудования в автомобильной промышленности, которые вкладывают средства в расширение технологической связи в транспортных средствах, и производители автономных транспортных средств, вероятно, будут затронуты этим руководством. Ответственность за выполнение этого руководства, вероятно, будет нести администрация Байдена и, в частности, Пит Буттиджиг, кандидат избранного президента Байдена на пост министра транспорта и бывший мэр Саут-Бенда, штат Индиана.

Всеобъемлющее законодательство о конфиденциальности

116-й Конгресс обещал принять федеральное законодательство о конфиденциальности. Председатель Сенатского комитета по торговле Роджер Уикер (R-Miss.) Представил Закон об установлении американских рамок для обеспечения доступа к данным, прозрачности и подотчетности (SAFE DATA Act) (S. 4626), и член рейтинга Мария Кантвелл (D-Wash.) представила Закон о правах потребителей в Интернете (COPRA) (S. 2968).). Эти законодательные предложения имеют много общих положений, таких как установление новых прав на неприкосновенность частной жизни для потребителей, но положения о принудительном исполнении остаются камнем преткновения. Таким образом, внимание к федеральному законодательству о конфиденциальности может вернуться в 2021 году. Эффективный контроль распространения вируса COVID-19

включал и будет включать отслеживание и отслеживание дел, которые требуют действий по сбору и обработке данных, которые повышают потенциальные риски конфиденциальности. Эти риски привлекли внимание федеральных законодателей и могут даже привести к требованиям как к государственным, так и к частным организациям, которые собирают и обрабатывают личные данные. Закон о конфиденциальности данных также может включать положения, регулирующие безопасность данных, уведомление об утечке данных, биометрические данные и искусственный интеллект.

Защитники конфиденциальности в администрации Байдена

Администрация Байдена, вероятно, вновь сосредоточит внимание на конфиденциальности и правоприменении, отчасти благодаря руководству избранным вице-президентом Харрис по этим вопросам, когда она работала Генеральным прокурором Калифорнии. В этой роли она была в авангарде обеспечения соблюдения законов штата о конфиденциальности и защите прав потребителей от предприятий, а также выпустила руководство по кибербезопасности, которое по-прежнему имеет влияние.

Считается, что избранные в кабинет министров и руководящие сотрудники администрации Байдена обладают необходимым аппетитом и опытом для поддержки программы обеспечения конфиденциальности потребителей. Например, нынешний генеральный прокурор Калифорнии Ксавье Бесерра, который был избран избранным президентом на должность секретаря Министерства здравоохранения и социальных служб США (HHS), руководил внедрением и соблюдением Закона Калифорнии о защите конфиденциальности потребителей (CCPA). Ожидаемый уход Бесерры может нарушить все еще новую повестку дня CCPA, назначений в новый административный орган штата, отвечающий за надзор за конфиденциальностью, и реализацию Закона о правах конфиденциальности Калифорнии (CPRA), недавно утвержденной меры голосования, которая вступает в силу 1 января 2023 г. Кроме того, который помогал разработать CCPA и призвал к реформе раздела 230 Закона о порядочности в коммуникациях, который обеспечивает защиту от ответственности онлайн-платформ.

Усиление нормативного правоприменения и надзора со стороны Конгресса

Если тенденция к назначению защитников конфиденциальности на руководящие должности в администрации Байдена сохранится, следует ожидать значительного увеличения количества принудительных мер. Федеральная торговая комиссия (FTC) недавно активизировала свои обзоры крупных технологических компаний, приказав таким компаниям объяснить, как они собирают и используют личные данные, и ожидается, что такие обзоры будут продолжены в 2021 году. Кроме того, FTC и 48 генеральных прокуроров подали отдельные иски в федеральном суде 16 декабря 2020 г., обвиняющие двух технологических гигантов в нарушениях антимонопольного законодательства, и почти 40 штатов подали антимонопольный иск17 декабря 2020 года. Учитывая недавнее обязательство штатов по изучению технологических гигантов, федеральное правительство может уступить контроль над этими вопросами во время административного перехода в Вашингтоне, округ Колумбия. В качестве альтернативы, эти действия штата могут стимулировать утверждение полномочий в отношении антимонопольного

законодательства и проблем конфиденциальности про «Big Tech» на федеральном уровне. Конгресс также продолжит осуществлять надзор за компаниями "крупных технологий", поскольку республиканцы и демократы заявили о своей приверженности решению проблем антимонопольного законодательства и конфиденциальности, которые у них возникают в отношении таких компаний.

Заключение

Хотя значительные изменения в кибербезопасности и конфиденциальности могут произойти не сразу, администрация Байдена и 117-й Конгресс, вероятно, примут значимые реформы, которые могут повлиять на транспортную отрасль. Пакет стимулов для инфраструктуры представляет собой наиболее привлекательный инструмент для транспортных реформ, связанных с кибербезопасностью, включая широкое развертывание широкополосной связи и расширение государственно-частных партнерств. Если у вас есть какие-либо вопросы об этих потенциальных реформах или вы хотите принять участие в решении этих вопросов, свяжитесь с авторами». ***(Marissa C. Serafino, Mark S. Melodia, Ashley L. Shively. Transportation Cybersecurity and Privacy Under Biden // Holland & Knight (https://www.hklaw.com/en/insights/publications/2021/01/transportation-cybersecurity-and-privacy-under-biden#page=1). 06.01.2021).***

***

«Согласно источникам, Энн Нойбергер присоединится к Совету национальной безопасности.

Избранный президент Джо Байден, как сообщается, привлек директора Агентства национальной безопасности по кибербезопасности для выполнения совершенно новой кибер-роли в своем Совете национальной безопасности.

По сообщению Politico, Энн Нойбергер, более 10 лет проработавшая в АНБ и его кибер-глава с 2019 года, станет заместителем советника по национальной безопасности страны по кибербезопасности.

Этот шаг повысит кибербезопасность до высшего приоритета для правительства США. Совет национальной безопасности является главным форумом президента для рассмотрения вопросов национальной безопасности и внешней политики с участием старших советников по национальной безопасности и должностных лиц кабинета министров.

Источники сообщили Politico, что Нойбергер, таким образом, будет отвечать за координацию кибербезопасности в агентствах и ведомствах федерального правительства. Одна из ее наиболее вероятных первых задач будет иметь дело с разрастающейся кибератакой SolarWinds, осуществленной хакерами из национальных государств, которые, как считается, поддерживаются Россией. Масштабы масштабной кампании все еще изучаются, и представители службы кибербезопасности в администрации Трампа уже заявили, что процесс исправления будет сложным, трудным и чрезвычайно дорогостоящим.

Нойбергер стала первым директором АНБ по кибербезопасности и заместителем национального менеджера в 2019 году, проработав пять лет на посту директора по рискам АНБ. Она отвечает за обмен информацией об угрозах между

АНБ и государственными и частными организациями, особенно в отношении угроз критически важной инфраструктуре. Роль АНБ в кибербезопасности США включает выполнение функций Управления национального менеджера (ONM) для систем, которые обрабатывают секретную информацию или иным образом имеют решающее значение для военной или разведывательной деятельности.

Предоставление кибербезопасности места за столом Совета национальной безопасности согласуется с заявленным интересом новой администрации Байдена в усилении позиции США в области кибербезопасности.

«Администрация Байдена-Харриса сделает кибербезопасность своим главным приоритетом, сделав ее императивом для всего правительства с первого дня», - сказал агентству СМИ переходный пресс-секретарь перехода Байдена. «Мы будем укреплять наши партнерские отношения с частным сектором, академическими кругами и гражданским обществом; подтвердить нашу приверженность международным нормам и участие в решении кибер-проблем; и расширять наши инвестиции в инфраструктуру и людей, которые нам нужны для эффективной защиты страны от злонамеренной кибер-активности». ***(Tara Seals. Biden to Appoint Cybersecurity Advisor to NSC – Report // Threatpost (https://threatpost.com/biden-cybersecurity-advisor-nsc/162867/). 07.01.2021).***

***

«Пользователи социальной сети Parler, которые участвовали в беспорядках на прошлой неделе в Капитолии США, по сообщениям, обеспокоены объявлением о том, что несколько хакеров-активистов заархивировали сообщения, которые происходили в режиме реального времени во время беспорядков, и что они будут публиковать сообщения для помощи правоохранительным органам в расследованиях. Другой хакер-активист, как сообщается, сказал, что она архивировала материалы во время их публикации, чтобы показать, как платформа использовалась для планирования атаки и для общения участников во время нападения.

Сообщается, что Парлер был популярным способом общения в течение месяцев, предшествовавших выборам прошлой осенью, после того как Facebook и Twitter начали проверять и маркировать контент, который был ложным или вводящим в заблуждение.

Один из хакеров-активистов утверждает, что она заархивировала 30 терабайт (30 000 гигабайт) общедоступных сообщений о событиях, приведших к беспорядкам и во время них, чтобы они были сохранены до того, как платформа будет отключена, что произошло в понедельник.

Некоторые из данных, которые были заархивированы, включают законно полученные данные GPS, когда сообщения были сделаны участниками беспорядков. Данные GPS показывают, что пользователи Parler размещали видео и фотографии, находясь внутри Капитолия, включая как палаты Конгресса, так и офисы некоторых политиков». ***(LINN FOSTER FREEDMAN. Activist Hackers Claim They Archived Parler Content Leading Up to Riots // Robinson+Cole (https://www.dataprivacyandsecurityinsider.com/2021/01/activist-hackers-claim-they-archived-parler-content-leading-up-to-riots/). 14.01.2021).***

***

«18 декабря 2020 года федеральные органы финансового регулирования совместно объявили о предлагаемом правиле. Это наложит новые и расширенные требования к отчетности для контролируемых банковских организаций, которые столкнулись с «инцидентом компьютерной безопасности», требуя уведомления в течение 36 часов о любом инциденте с компьютерной безопасностью, который достигает уровня «инцидента с уведомлением». При значительном отклонении от текущих требований к отчетности для финансовых учреждений, которые столкнулись с инцидентом безопасности, предлагаемое правило в целом потребует уведомления о любом инциденте, который может повлиять на способность организации предоставлять услуги существенной части ее клиентской базы, ставя под угрозу жизнеспособность ключевых операции банковской организации или влияние на стабильность финансового сектора, независимо от типа или количества затронутой информации.

Предлагаемое правило было объявлено совместно Управлением финансового контролера, Казначейства (OCC), Советом управляющих Федеральной резервной системы («Совет») и Федеральной корпорацией страхования депозитов (FDIC). Ниже мы изложили основные выводы из Уведомления о предлагаемом нормотворчестве (NPR).

Организации, подпадающие под новые требования

Предлагаемое правило будет применяться к контролируемым банковским организациям и поставщикам банковских услуг, как описано в NPR:

Банковские организации будут включать следующие организации, в зависимости от соответствующего надзорного регулирующего органа:

Для OCC «банковские организации» будут включать национальные банки, федеральные сберегательные ассоциации, а также федеральные агентства и агентства.

По мнению Совета, «банковские организации будут включать все холдинговые банковские компании США и холдинговые ссудно-сберегательные компании; банки государств-членов; операции иностранных банковских организаций в США; Крайние и договорные корпорации.

Для FDIC «банковские организации» будут включать все застрахованные государственные банки, не являющиеся членами, застрахованные лицензированные государством филиалы иностранных банков и государственные сберегательные ассоциации.

Поставщики банковских услуг будут включать организации, которые предоставляют услуги, подпадающие под действие Закона о компаниях, оказывающих банковские услуги (BSCA), включая, помимо прочего, подготовку и отправку чеков, выписок, уведомлений и аналогичных предметов или любые другие канцелярские, бухгалтерские, бухгалтерские, статистические или аналогичные функции, выполняемые для депозитарного учреждения.

Предлагаемые требования к отчетности для «уведомительных инцидентов»

Предлагаемое правило требует, чтобы банковские организации уведомляли свой основной федеральный регулирующий орган в случае «инцидента с уведомлением».

Инцидент уведомления является «инцидентом компьютерной безопасности», что банковская организация считает, добросовестно может существенно нарушить, деградирует, или отрицательно влияют (я) способность банковской организации осуществлять банковские операции, деятельность или процессы, или предоставлять банковский продукты и услуги для существенной части его клиентской базы в ходе обычной деятельности; (ii) любое направление деятельности банковской организации, включая связанные с ней операции, услуги, функции и поддержку, и может привести к существенной потере выручки, прибыли или стоимости франшизы; или (iii) те операции банковской организации, включая связанные с ними услуги, функции и поддержку, в зависимости от обстоятельств, отказ или прекращение которых может создать угрозу финансовой стабильности Соединенных Штатов.

Предлагаемое правило определяет «инцидент компьютерной безопасности» как событие, которое (i) приводит к фактическому или потенциальному ущербу для конфиденциальности, целостности или доступности информационной системы или информации, которую система обрабатывает, хранит или передает; или (ii) представляет собой нарушение или неминуемую угрозу нарушения политик безопасности, процедур безопасности или политик допустимого использования.

Банковские организации должны будут уведомить свой основной федеральный регулирующий орган как можно скорее, но не позднее, чем через 36 часов после того, как банковская организация добросовестно считает, что произошел инцидент с уведомлением.

Расширение текущих требований к отчетности

Предлагаемое правило явилось бы заметным отходом от текущих федеральных требований к отчетности для финансовых учреждений в соответствии с Законом о банковской тайне (BSA) и Законом Грэмма-Лича-Блили (GLBA). NPR объясняет, что на высоком уровне, в соответствии с BSA, банковские организации могут быть обязаны сообщать об определенных кибер-событиях путем подачи отчета о подозрительной деятельности (SAR), если деятельность может быть связана с отмыванием денег. Организации также могут быть обязаны уведомлять федеральные регулирующие органы и отдельных лиц об инцидентах безопасности в соответствии с Межведомственным руководством по программам реагирования на несанкционированный доступ к информации о клиенте и Уведомлением о клиенте, которое интерпретирует Раздел 501 (b) GLBA, но такое уведомление будет инициировано только в том случае, если организации становится известно об инциденте, связанном с несанкционированным доступом или использованием, «Конфиденциальная информация о клиентах». NPR отмечает, что, хотя текущие требования к отчетности в соответствии с BSA и GLBA «могут предоставить агентствам уведомление об определенных инцидентах компьютерной безопасности», требования «слишком узки по своему охвату, чтобы рассматривать все соответствующие инциденты компьютерной безопасности, которые будут охвачены предлагаемое правило».

Примечательно, что предлагаемое правило потребует от банковских организаций также сообщать «об инцидентах, которые нарушают работу, но не ставят под угрозу конфиденциальную информацию о клиентах». Примеры, представленные NPR, включают крупномасштабные распределенные атаки типа «отказ в обслуживании», которые нарушают доступ к учетным записям клиентов, и неудачное обновление системы, которое приводит к массовым отключениям пользователей. Связывая требование об уведомлении с порогом существенности, предлагаемое правило в некоторой степени будет следовать модели, установленной Постановлением о кибербезопасности Департамента финансовых услуг Нью-Йорка, которое требует от учреждений, регулируемых Департаментом, уведомлять о любом событии кибербезопасности, которое имеет «разумная вероятность причинения материального ущерба какой-либо материальной части при нормальной работе» в течение 72 часов.

Жесткий график отчетности

Установив требование об уведомлении за 36 часов для контролируемых банковских организаций и поставщиков банковских услуг, федеральные органы финансового регулирования отмечают, что предлагаемое правило станет важным источником своевременной информации, связанной с угрозами, что «текущие требования к отчетности, связанные с киберинцидентами, не разработаны. и не собирался предоставлять». Хотя такие короткие сроки уведомления могут создать особую проблему для банков, столкнувшихся со сложными инцидентами безопасности, особенно с учетом того, что любая доступная техническая информация, вероятно, будет неполной или ненадежной в первые дни после инцидента, NPR отмечает, что агентства «не ожидают, что банковская организация обычно может определить, что инцидент с уведомлением произошел, сразу после того, как узнает об инциденте, связанном с компьютерной безопасностью». Вместо, агентства ожидают, что организация потратит «разумное количество времени», чтобы определить, что произошел инцидент с уведомлением, а затем уведомить свой основной регулирующий орган в течение 36 часов с момента вынесения такого определения. Ожидается, что банковские организации будут делиться только общей информацией о том, что известно на тот момент, и уведомление может быть предоставлено посредством любой формы письменного или устного общения.

Требования к уведомлениям для поставщиков банковских услуг

Помимо банковских организаций предлагаемое правило также налагает новые требования на поставщиков банковских услуг. Поставщики банковских услуг должны будут уведомить «как минимум двух лиц» в затронутом банке «сразу после того, как поставщик банковских услуг столкнется с инцидентом компьютерной безопасности, который, как он добросовестно считает, может нарушить, ухудшить или нанести ущерб услугам» в течение четырех часов или более. После получения такого уведомления, если банковская организация определяет, что произошел инцидент с уведомлением, банковская организация должна будет уведомить своего основного федерального регулирующего органа.

Предлагаемый регламент будет открыт для комментариев в течение 90 дней с момента его публикации в Федеральном реестре». ***(Kimberly Peretti, Emily Poole,***

Michael Youn. Financial Regulatory Agencies Announce Proposed Rule Requiring Notice of Computer Security Incidents // Alston & Bird (https://www.alstonprivacy.com/financial-regulatory-agencies-announce-proposed-rule-requiring-notice-of-computer-security-incidents/). 12.01.2021).

***

«Административная конференция судов США уполномочила федеральные окружные суды разработать политику приема «особо конфиденциальных судебных документов (HSD)», которые обычно подаются в электронном виде с печатью на бумаге. В заявлении Административной конференции также признается, что недавняя кибербезопасная атака на продукты SolarWinds поставила под угрозу конфиденциальность документов, хранящихся за печатью в Системе управления делами / электронных дел судебных органов (CM / ECF).

В результате суды по всей стране выпускают уведомления, определяющие, что составляет HSD, и как стороны должны подавать HSD, вступающие в силу немедленно. В то время как некоторые суды еще не выпустили руководящих указаний, ряд других федеральных судов издали общие постановления, требующие, чтобы HSD были поданы в бумажном виде в ящики для хранения документов в судах или за их пределами. Отдельным судам остается разделение между обработкой всех запечатанных документов как HSD и предоставлением председательствующему судье или, если его нет, главному судье, определение того, является ли документ HSD. Окружной суд США округа Колумбия будет придерживаться последнего подхода и при условии, что определение HSD может рассмотреть вопрос о том, содержит ли документ коммерческую тайну или конфиденциальную правительственную информацию о правоприменении.

На практическом уровне эти приказы могут потребовать, чтобы запечатанные документы, включая протесты на торгах, были поданы до закрытия судебных заседаний, чтобы считаться поданными своевременно, а не в 23:59, крайний срок для электронной подачи. Приказы также могут потребовать проведения дополнительных конференций между сторонами для достижения консенсуса по поводу того, какая информация должна храниться под печатью, особенно если председательствующий судья или главный судья округа должен решить, когда стороны не могут прийти к согласию, как это часто бывает. Мы продолжим следить за этим развитием». ***(Steve McBrady, Brian Tully McLaughlin, Lyndsay Gorton, Alexandra Barbee-Garrett. Cybersecurity Breach Turns Back the Clock – Confidential Information to be Filed in Paper // Crowell & Moring LLP (https://www.governmentcontractslegalforum.com/2021/01/articles/cybersecurity/cybersecurity-breach-turns-back-the-clock-confidential-information-to-be-filed-in-paper/#page=1). 12.01.2021).***

***

«11 декабря 2020 года Конгресс представил президенту Трампу HR 6395, Закон о полномочиях национальной обороны на 2021 финансовый год. 23 декабря 2020 года президент Трамп наложил вето на закон. Впоследствии Палата

представителей проголосовала 28 декабря 2020 года, а Сенат 1 января 2021 года проголосовал за отмену вето.

Этот закон содержит множество положений, которые налагают новые требования, ожидания или возможности для государственных подрядчиков. Группа по государственным контрактам Crowell & Moring обсуждает наиболее важные изменения в NDAA на 2021 финансовый год для государственных подрядчиков.

Кибербезопасность

NDAA на 2021 финансовый год заметно изобилует мерами кибербезопасности, особенно теми, которые направлены на укрепление позиции кибербезопасности оборонной промышленной базы (DIB). Меры кибербезопасности включают:

Раздел 1260F устанавливает оценку эффективности текущей Национальной киберстратегии, которая направлена на предотвращение промышленного шпионажа и киберхищения интеллектуальной собственности и личной информации Китайской Народной Республикой.

Раздел 1712 устанавливает требования для каждой основной системы вооружения, которая должна быть оценена на предмет кибер-уязвимостей и для определения приоритетных критических инфраструктур по широким областям применения систем оружия. В этом разделе также создается Стратегическая программа кибербезопасности для улучшения систем, критической инфраструктуры, цепей уничтожения и процессов, связанных с ядерным сдерживанием и нанесением ударов, определенными задачами нанесения ударов с применением обычных средств дальнего действия, наступательными кибероперациями и противоракетной обороной страны.

Раздел 1714 обновляет Комиссию по киберпространству солярия, которая стала влиятельной в разработке подходов к кибербезопасности для защиты Соединенных Штатов от кибератак.

Раздел 1716 наделяет Агентство кибербезопасности и безопасности инфраструктуры (CISA) Министерства внутренней безопасности (DHS) полномочиями выдавать административные повестки поставщикам интернет-услуг, когда оно обнаруживает критические уязвимости безопасности инфраструктуры, но не может обнаружить владельца.

Раздел 1735 позволяет Министерству обороны (DoD) интегрировать возможности и системы для мониторинга активности пользователей, а также для кибербезопасности конечных точек и сбора метаданных о сетевой активности. Цель состоит в том, чтобы обеспечить взаимную поддержку и обмен информацией. В разделе также содержится призыв к Министерству обороны рассмотреть возможность использования экземпляров платформы больших данных, на которых размещены метаданные кибербезопасности, для хранения и анализа всех данных мониторинга активности, собранных в Министерстве обороны.

Раздел 1736 позволяет Министерству обороны провести оценку выполнимости и ресурсов, необходимых для создания программы архитектуры датчиков кибербезопасности DIB, ответственной за развертывание готовых коммерческих решений для мониторинга открытой поверхности интернет-атак DIB. Министерство обороны разработает структуру управления, которая позволит

собирать данные о кибербезопасности на открытых поверхностях интернет-атак подрядчиков DIB способом, совместимым с (1) существующими или будущими возможностями Департамента для анализа и (2) инструментами. и сбор, при необходимости, данных о кибербезопасности в информационной сети Департамента.

Раздел 1737 требует, чтобы Министерство обороны провело оценку осуществимости и ресурсов, необходимых для создания программы обмена информацией об угрозах DIB. В рамках программы этот раздел ставит перед Министерством обороны задачу:

Установите конкретные согласованные временные рамки для всех категорий сообщений об инцидентах кибербезопасности; и

Создайте единую информационную службу для всех обязательных отчетов об инцидентах кибербезопасности в Департамент, включая инциденты, связанные с контролируемой несекретной информацией (CUI) и секретной информацией.

Раздел 1739 требует, чтобы Министерство обороны провело оценку выполнимости и ресурсов, необходимых для создания Программы поиска угроз кибербезопасности DIB для активного выявления уязвимостей кибербезопасности в DIB. В этом разделе указано, что оценка будет оценивать, среди прочего:

Элементы поиска угроз, необходимые для подрядчиков в соответствии с Сертификацией модели зрелости кибербезопасности (CMMC), включая методы, относящиеся к непрерывному мониторингу, обнаружению и расследованию аномальной активности, указывающей на инцидент кибербезопасности.

Пригодность непрерывной программы поиска угроз кибербезопасности в качестве дополнения к требованиям CMMC, которая будет учитывать: (i) сбор и анализ метаданных о сетевой активности для обнаружения возможных вторжений; (ii) быстрое расследование и устранение возможных вторжений; (iii) Требования к снижению любых уязвимостей, выявленных в соответствии с программой поиска угроз кибербезопасности; и (iv) Механизмы, позволяющие Министерству обороны обмениваться вредоносным кодом в DIB, индикаторами компрометации (IOC) и аналитическими сведениями о меняющемся ландшафте угроз.

Участие генеральных подрядчиков и субподрядчиков в программе поиска угроз кибербезопасности. Министерство обороны рассматривает запреты на закупки для подрядчика, не соблюдающего будущую программу поиска угроз.

Степень, в которой подрядчику может потребоваться участие в программе поиска угроз, может зависеть от характера и объема CUI, обрабатываемых в соответствии с контрактом DoD.

Раздел 1742 требует, чтобы Министерство обороны оценивало каждый компонент Департамента в соответствии со структурой CMMC и представляло в Конгресс отчет по защите относительно полученных результатов. Компоненты будут оцениваться по CMMC Уровня 3 или выше.

Раздел 3131 поощряет Администратора по физической ядерной безопасности установить процедуры, требующие от подрядчиков и субподрядчиков сообщать в течение 60 дней с момента обнаружения главному информационному директору, когда в защищенную сеть подрядчика или субподрядчика Министерства энергетики оказывается успешное проникновение.

Государственные контракты на интеллектуальную собственность

Раздел 804 требует, чтобы Министерство обороны издало правила и инструкции для облегчения доступа Министерства обороны к интерфейсам модульной системы и их использования. Положения и руководства, в соответствующей части, должны включать требования, которые:

Программный офицер для каждой системы вооружения характеризует желаемую модульность системы вооружения, за которую отвечает программный офицер; и

Каждый контракт, следующий за реализацией правил и руководств, включает требования к поставке интерфейсов для модульных систем, которые считаются важными в стратегии приобретения или документации.

Правила и руководство применяются к любому программному офису, ответственному за создание прототипа, приобретение или поддержание новой или существующей системы вооружения, и могут быть распространены на программные невооруженные системы, включая бизнес-системы и системы кибербезопасности, через год после принятия постановлений. реализуются, но не через два года после внедрения.

Раздел 804 также вносит поправки в 10 USC § 2446a, чтобы расширить требование об использовании модульных открытых систем в максимально возможной степени для программ, выходящих за рамки основных программ оборонных закупок. Раздел 804 также вносит поправки в 10 USC § 2320, чтобы предоставить правительственным целям права на интерфейсы модульных систем, разработанные исключительно за частные или частично за счет федеральных средств. Раздел 804 также требует от Министерства обороны США создать центральный репозиторий для интерфейсов и соответствующей документации и предоставить доступ к такому репозиторию правительственным и негосударственным организациям в соответствии с схемами прав, установленными 10 USC § 2320.

Раздел 839 требует, чтобы Счетная палата правительства (GAO) представила в Конгресс до 1 октября 2021 г. отчет с оценкой выполнения Министерством обороны Инструкции 5010.44 «Приобретение интеллектуальной собственности и лицензирование», включая, в соответствующей части:

Степень, в которой DoD выполняет основные принципы, установленные в Инструкции;

Влияние выполнения Инструкции на отдельные приобретения; и

Прогресс Министерства обороны в создании штата экспертов по интеллектуальной собственности в соответствии с требованиями 10 USC § 2322.

Другие транзакции (OTs)

Раздел 833 требует, чтобы Министерство обороны опубликовало список консорциумов органов OT, используемых для распространения возможностей заключения контрактов с OT. Этот список облегчит компаниям поиск соответствующих консорциумов и, в свою очередь, потенциальных проектов.

Раздел 1752 наделяет недавно созданного Национального кибердиректора полномочиями заключать контракты и OT, если это необходимо для выполнения обязанностей Управления национального кибердиректора. Этот раздел, наряду с

Разделом 5301 ниже, отражает продолжающиеся усилия Конгресса по расширению использования ОТ.

Раздел 2866 (c) (1) требует, чтобы министр армии разработал пилотную программу для разработки и использования онлайн-инструмента инвентаризации недвижимости для определения существующего пространства, доступного на объектах армии. Положение прямо требует от армии рассмотреть новаторские подходы, включая использование ОТ и коммерческих готовых технологий, для этой программы.

Раздел 5301 разрешает Национальному институту стандартов и технологий (NIST) использовать ОТ, среди прочего, для поддержки измерительных исследований и разработки передовых практик и стандартов для искусственного интеллекта (AI), создания наборов данных для исследований, разработки и использования AI.; и разработать добровольные консенсусные стандарты и руководящие принципы для надежных систем ИИ.

Раздел 9903 предписывает Министерству обороны установить государственно-частное партнерство, чтобы стимулировать создание одного или нескольких консорциумов с целью обеспечения разработки и производства безопасной микроэлектроники (включая интегральные схемы, логические устройства, память, а также упаковку и тестирование для того же). Это положение разрешает Министерству обороны использовать ОТ, а также другие средства для стимулирования внутреннего развития производства микроэлектроники, а также научно-исследовательских и опытно-конструкторских разработок. Раздел 9903 налагает определенные условия на типы предприятий, которые могут участвовать, например, требует, чтобы участники обладали процессами управления для выявления и снижения рисков безопасности цепочки поставок, например, история государственных контрактов; уязвимости цепочки поставок; иностранная собственность, контроль или влияние).

Национальная безопасность

Учитывая текущую политическую направленность на обеспечение безопасности критически важных цепочек поставок в США, кибербезопасность и потенциальные уязвимости, связанные с иностранным владением, контролем или влиянием (FOCI), существует множество статей, связанных с оценкой рисков национальной безопасности и мерами по их смягчению, а также с отчетностью и предпочтениями или ограничениями источников.

Раздел 819 вносит поправки в Раздел 847 NDAA на 2020 финансовый год, который требует от покрываемых подрядчиков и субподрядчиков (компаний с некоммерческим контрактом или субподрядом на сумму, превышающую $ 5 000 000) раскрывать информацию о бенефициарном владении и контроле, а Министерство обороны должно выполнять FOCI. оценка рисков как часть определения ответственности. Новый раздел 819 вносит поправки в предыдущий раздел, требуя от Министерства обороны периодически оценивать соблюдение подрядчиком требований к раскрытию информации о свободе информации, создавать процедуры для рассмотрения соответствующих изменений в праве собственности и внедрять Раздел 847 с помощью пересмотренных политик и обучения до 1 июля 2021 года.

Раздел 835 требует от Министерства обороны разработать требования к критериям безопасности программного обеспечения, которые должны быть включены в заявки на коммерческие и разрабатываемые программные решения и оценку заявок, а также разработать процедуры проверки безопасности кода в координации с усилиями по кибербезопасности.

Раздел 837 требует от Министерства обороны США определения политик и процедур для защиты интеллектуальной собственности США, технологий и других данных и информации (включая оборудование и программное обеспечение), имеющих отношение к обороне, от приобретения правительством Китая, и, если существующие политики и процедуры являются недостаточными, разработать дополнительные политики и процедуры. Раздел также требует от Министерства обороны рассмотреть механизмы ограничения нынешних или бывших сотрудников подрядчиков или субподрядчиков (на любом уровне), которые вносят значительный и существенный вклад в любую критически важную технологию национальной безопасности, от работы непосредственно на компании, находящиеся в собственности, под контролем или под влиянием правительства Китай.

Раздел 841 вносит поправки в 10 USC § 2533c (запрет на приобретение чувствительных материалов из стран, не являющихся союзниками), добавляя с 1 января 2023 г. ограничение на приобретение Министерством обороны США покрытых печатных плат (любых частично изготовленных или полностью изготовленных неизолированных печатных плат или полностью или частично собранная печатная плата, которая выполняет критически важную функцию в любом продукте или услуге, которая не является коммерческим продуктом или коммерческой услугой) из страны, на которую распространяется действие гарантии (Северная Корея, Китай, Россия, Иран). Кроме того, Министерство обороны должно оценить преимущества и риски расширения запрета на включение печатных плат в коммерческие продукты или услуги или в продукты или услуги COTS.

Раздел 848 требует от Министерства обороны в максимально возможной степени приобретать стратегические и критически важные материалы, необходимые для удовлетворения оборонных, промышленных и основных гражданских потребностей Соединенных Штатов в порядке предпочтения: (1) из источников, расположенных в США; (2) из источников, расположенных в пределах национальной технологической и промышленной базы (NTIB, определенный в 10 USC § 2500); или (3) из других источников в зависимости от обстоятельств.

Раздел 885 изменяет 41 USC § 2313 (d), требуя раскрытия бенефициарной собственности в базе данных, поддерживаемой GSA, с информацией о подрядчиках и получателях грантов с контрактом с федеральным агентством или грантом на сумму, превышающую 500 000 долларов. Этот раздел тесно связан с разделом 6403, который обновляет требования к отчетности по борьбе с отмыванием денег, чтобы включить в него отчетность о бенефициарной собственности для определенных компаний как часть любого предложения или предложения по контракту сверх упрощенного порога приобретения.

Раздел 9202 создает «Инновационный фонд государственных беспроводных цепочек поставок» для предоставления грантов на конкурсной основе для поддержки продвижения и развертывания сетей связи 5G и последующих сетей, а также интеграции и безопасности сетей от разных поставщиков, среди прочего. Раздел также создает «Многосторонний фонд безопасности электросвязи» для поддержки разработки и внедрения безопасных телекоммуникационных технологий.

Раздел 9905 учреждает «Многосторонний фонд безопасности полупроводников», который будет создан в сотрудничестве с иностранными партнерами для поддержки разработки и внедрения измеримых безопасных полупроводников и измеримых безопасных цепочек поставок полупроводников.

TINA и бизнес-системы

Раздел 806 заменяет термин «значительный недостаток» и его определение в Разделе 893 NDAA на 2011 финансовый год. Ранее этот термин определялся как «недостаток в системе, который существенно влияет на способность должностных лиц Министерства обороны и подрядчика полагаться на информацию, производимую системой, которая необходима для целей управления». Комиссия по разделу 809 в своем отчете за январь 2019 года выразила обеспокоенность тем, что термин «значительный недостаток» и его определение несовместимы с двухуровневой характеристикой недостатков внутреннего контроля, используемой в общепринятых стандартах аудита, что создает путаницу в отношении серьезности недостатков. определены в бизнес-системах подрядчика. Как таковой, Комиссия рекомендовала заменить термин «значительный недостаток» определением «существенной слабости», которое дает частный сектор. NDAA на 2021 финансовый год признает и следует рекомендациям комиссии, заменяя «существенные недостатки» на «существенные недостатки» и по существу принимая определение «существенной слабости» частного сектора, предложенное комиссией - «недостаток или недостаток». сочетание недостатков во внутреннем контроле информации в бизнес-системах подрядчика, так что существует разумная вероятность [вероятная или более чем маловероятная, но менее вероятная] того, что существенное искажение такой информации не будет предотвращено или обнаружено и исправлено на своевременная основа».

Раздел 814 вносит поправки в 10 USC § 2306a, устанавливая стандартный порог в 2 миллиона долларов для применения требований в отношении сертифицированных данных о стоимости или ценах в соответствии с положениями «Правдивость переговоров / достоверные данные о стоимости или ценах». В частности, поправка удаляет различные конкретные и сопряженные требования, включая ограничения по срокам и разные пороговые значения в долларах, которые возникли в результате повышения порогового значения в 2018 году, и вместо этого устанавливает последовательный триггер в размере 2 миллионов долларов США для требования сертифицированных данных о стоимости или ценах для всех основных контрактов, заключенных на или после 1 июля 2018 г., а также для всех заключенных субконтрактов и внесенных изменений (для первичного или субподрядного) 1 июля 2018 г. или после этой даты, независимо от даты присуждения основного контракта. К тому же,

Коммерческие продукты и услуги

Раздел 816 изменяет установленные законом процедуры определения коммерческих продуктов и коммерческих услуг, выполняемые сотрудниками Министерства обороны США по контрактам. Эти изменения предназначены для обеспечения большей согласованности при определении коммерческой ценности в Департаменте. В законопроект Палаты представителей были внесены более серьезные изменения, которые увеличили бы нагрузку на сотрудников по контрактам, стремящихся отклониться от предыдущих определений коммерческой деятельности, и расширили бы презумпцию коммерции на компоненты коммерческих продуктов. В конце концов, однако, Конгресс решил пойти на более скромные изменения. Раздел 816 вносит поправки в 10 USC § 2380, чтобы уточнить, что при принятии решения сотрудник по контракту может как (1) запросить поддержку у Агентства по управлению оборонными контрактами, Агентства по аудиту оборонных контрактов и других экспертов Департамента; и (2) учитывать мнения организаций государственного и частного секторов. Раздел 816 также устанавливает, что сотрудник по контракту должен задокументировать решение в письменном меморандуме, включая подробное обоснование, в течение 30 дней с момента присуждения контракта.

Соглашения о неразглашении

Раздел 883 запрещает Министерству обороны присуждать контракт, если подрядчик не заявляет, что (i) он не требует от своих сотрудников подписывать внутренние соглашения или заявления о конфиденциальности, которые запрещают или иным образом ограничивают таких сотрудников в законном сообщении о растрате, мошенничестве или злоупотреблениях, связанных с выполнение контракта DoD, и (ii) он проинформирует своих сотрудников об ограничениях таких соглашений о конфиденциальности. В настоящее время FAR 52.203-19…». ***(National Defense Authorization Act for Fiscal Year 2021: Need-to-Know Provisions for Government Contractors // Crowell & Moring LLP (https://www.crowell.com/NewsEvents/AlertsNewsletters/all/National-Defense-Authorization-Act-for-Fiscal-Year-2021-Need-to-Know-Provisions-for-Government-Contractors). 12.01.2021).***

***

«Как показывает недавняя атака SolarWinds Orion, кибербезопасность в ближайшие годы будет в центре внимания как государственных, так и негосударственных организаций. В сообществе федеральных подрядчиков давно прогнозировалось, что повышенные правительственные требования к кибербезопасности в конечном итоге приведут к соответствующему увеличению количества судебных разбирательств по Закону о ложных исках (FCA), связанных с соблюдением требований кибербезопасности. Этот прогноз может вскоре оказаться верным, поскольку в речи заместителя помощника генерального прокурора Майкла Гранстона в декабре 2020 г. «Мошенничество, связанное с кибербезопасностью» как «область, в которой мы могли бы увидеть усиление деятельности Закона о ложных исках». В этом посте обсуждаются недавние попытки использовать FCA

для обеспечения соблюдения требований кибербезопасности - и, исходя из этих усилий, то, что правительственные подрядчики могут ожидать увидеть в будущем.

В последние годы правительство и истцы qui tam начали использовать FCA для преследования предполагаемого несоблюдения правил кибербезопасности, и некоторые из этих усилий получили поддержку. Например, в мае 2019 года федеральный окружной суд в Калифорнии отказался закрыть дело, утверждая, что государственный подрядчик ложно подтвердил свое соответствие стандартам кибербезопасности при заключении контрактов с Министерством обороны. А в июле 2019 года Министерство юстиции объявило, что другой подрядчик согласился выплатить более 8 миллионов долларов в связи с урегулированием иска qui tam о несоблюдении федеральных стандартов кибербезопасности, что стало первым урегулированием, основанным на утверждениях FCA о несоблюдении требований кибербезопасности.

Однако недавно, по крайней мере, один суд отклонил попытку построить дело FCA на основании предполагаемых отклонений от правил кибербезопасности. В октябре 2020 года федеральный окружной суд округа Колумбия отклонил иск qui tam, в котором утверждалось, что подрядчик не раскрыл уязвимость системы безопасности в компьютерных системах, которые он продал Соединенным Штатам. США экс отн. Адамс против Dell Computer Corp., 15-cv-608 (DDC 8 октября 2020 г.). Отклонение суда было основано на его выводе о том, что информатор не смог доказать, что несоблюдение было «существенным». Как отметил суд, «ссылка на технологическую политику не требуют бездефектных продуктов», и что любую применимую политику безопасности можно было бы вместо этого решить, «предоставив необходимую помощь для устранения или уменьшения уязвимостей по мере их появления».

Мы ожидаем, что в будущем строгие требования FCA к существенности будут по-прежнему создавать серьезное препятствие для истцов в будущих делах, предполагающих несоблюдение все более подробных правил кибербезопасности. Однако, как предвещает недавняя речь г-на Гранстона, федеральное правительство и истцы qui tam готовы подать иски в соответствии с FCA на основании обвинений в несоблюдении требований кибербезопасности. Хотя эти обвинения могут принимать множество форм, в частности, есть два нормативных нововведения, которые могут дать повод для беспокойства предприимчивым информаторам и создать риск FCA для неосторожных подрядчиков. Во-первых, в соответствии с методологией оценки NIST 800-171 DoDМинистерство обороны теперь требует, чтобы подрядчики выполняли предварительную самооценку (известную как «Базовая оценка») своего соответствия 110 мерам безопасности, указанным в NIST 800-171. Результатом этой базовой оценки является числовой балл, который предоставляется правительству, и дата, к которой подрядчик представляет, что он будет в полном соответствии со всеми средствами контроля NIST 800-171. После присуждения награды Министерство обороны может принять решение о проведении своей собственной средней оценки (посредством бумажной проверки) или высокой оценки (посредством личной проверки) соответствия подрядчика требованиям безопасности NIST 800-171.

Этот процесс оценки может вызвать разногласия между подрядчиком и правительством по поводу того, в какой степени подрядчик соблюдает меры безопасности NIST 800-171. В частности, большое несоответствие между числовым баллом базовой оценки и числовым баллом средней или высокой оценки может привести к утверждениям о том, что подрядчик не смог точно представить свои требования к кибербезопасности, тем самым увеличивая риск FCA.

Во-вторых, оборонным подрядчикам вскоре будет предложено получить и предоставить сертификат модели зрелости кибербезопасности (CMMC) от аккредитованной сторонней организации по оценке CMMC. Ожидается, что в рамках этого процесса сертификации подрядчики продемонстрируют свою способность соответствовать требованиям безопасности NIST 800-171, а также нескольким дополнительным мерам безопасности. Обвинения несоответствия между самооценкой соответствия 800-171 и оценкой третьей стороны CMMC, также могут привлечь внимание потенциальной Qui Tam истцов.

Однако, это может оказаться трудным для правительства или Qui TAM истцы установить ответственность FCA на основе утверждений о кибербезопасности несоблюдения. Во-первых, как отмечалось выше, ответственность FCA может быть наложена только в том случае, если требуется «существенное», Что означает, что несоблюдение требований будет иметь «естественную тенденцию влиять или может повлиять» на решение правительства о выплате подрядчику. Однако федеральные контракты часто содержат требования к кибербезопасности среди десятков, если не сотен, других нормативных обязательств. Во многих случаях маловероятно, что решение правительства о выплате подрядчику будет зависеть от строгого соблюдения определенного контроля кибербезопасности или набора средств контроля, и в этом случае несоблюдение этого контроля не будет «существенным».

Во-вторых, ответственность FCA требует доказательства того, что несоблюдение было «знанием», что означает, что подрядчик действительно знал, что он не соблюдает требование, действовал с умышленным невежеством или действовал с безрассудным пренебрежением. Однако многие требования кибербезопасности являются новыми и сформулированы широко, что допускает разумные различия в технической интерпретации. Существует существенная судебная практика, устанавливающая, что подрядчик не может нести ответственность в соответствии с FCA за разумное и добросовестное прочтение нечетких нормативных требований.

Таким образом, даже если прогнозы о росте числа дел о кибербезопасности FCA сбудутся, есть веские основания полагать, что многие такие дела столкнутся со значительными встречными ветрами. Хотя все дела различаются, стандартные средства защиты по таким вопросам будут полностью доступны, включая как материально-правовые защиты, подобные тем, которые описаны выше, так и процедурные средства защиты, такие как установленный законом запрет публичного раскрытия информации. Тем не менее, вероятность увеличения количества случаев FCA подчеркивает важность обеспечения внимательного отношения к соблюдению требований кибербезопасности и связанных с ними заявлений». ***(Michael Wagner, Peter B. Hutt II, Susan B. Cassidy, Andrew Guy.***

Cybersecurity and Government Contracting: False Claims Act Considerations // COVINGTON & BURLING LLP (https://www.insidegovernmentcontracts.com/2021/01/cybersecurity-and-government-contracting-false-claims-act-considerations/#page=1). 11.01.2021).

***

«Арканзасский университет в Литл-Роке в партнерстве с Forge Institute и Арканзасским университетом в Фейетвилле продвигает прикладные исследования в областях, поддерживающих национальную оборону, включая кибербезопасность.

Это партнерство является первой в своем роде возможностью в Арканзасе и приведет к конкурентным исследованиям, возможностям сотрудничества и создаст платформу для экономического роста и создания рабочих мест.

Партнерство будет сосредоточено на защитных возможностях кибербезопасности нового поколения для промышленных систем управления (ICS / SCADA) с целью дальнейшей защиты критически важной инфраструктуры страны.

Первыми сотрудниками университета будут Филип Хафф, доцент кафедры кибербезопасности в UA Little Rock, и доктор Крис Фарнелл, управляющий директор испытательного стенда Национального центра надежной передачи электроэнергии (NCREPT) в Университете А.

«Центр развивающейся аналитики в UA Little Rock работает с Forge Institute более года, - сказал Хафф. «Мы рады расширить эти совместные усилия для работы над некоторыми из самых сложных национальных проблем искусственного интеллекта в области кибербезопасности. Это сотрудничество откроет доступ к возможностям прикладных исследований для студентов и преподавателей из Арканзаса».

Совместная команда будет использовать возможности кибер-тренажерного зала UA Little Rock Cyber Gym, испытательного стенда Национального центра надежной передачи электроэнергии (NCREPT) в Соединенном Королевстве, а также профессиональную и опытную команду и возможности Forge Institute. UA Little Rock и U of A определены Агентством национальной безопасности и Министерством внутренней безопасности США в качестве академических центров передового опыта. Университет А также является центром передового опыта Министерства энергетики США.

Это сотрудничество объединяет лучшие ресурсы, исследования и возможности UA Little Rock и U of A, а также уникальные возможности и взаимоотношения Forge Institute. Forge Institute будет сотрудничать с ключевыми исследователями, чтобы предоставить доступ к уникальным исследовательским возможностям в поддержку национальной обороны.

«Мы рады сотрудничать с UA Little Rock и UA Fayetteville в разработке инновационных решений, которые помогут решить сложные и растущие проблемы кибербезопасности и национальной безопасности нашей страны», - сказал Ли Уотсон, председатель и главный исполнительный директор Forge Institute. «Подключаясь к существующему кибернетическому и оборонному сектору штата и опираясь на него, мы создаем основу для внедрения инноваций, которые напрямую

приведут к созданию высокооплачиваемых рабочих мест для жителей штата Арканзас. Я очень рад этому сотрудничеству и тому, как оно поможет нашему штату и стране лучше защищаться от продвинутых киберпреступников и способствовать росту экономики штата». ***(UA Little Rock partners with Forge Institute, U of A to Advance Applied Research In Cybersecurity to Support National Defense // Newswise (https://www.newswise.com/articles/ua-little-rock-partners-with-forge-institute-u-of-a-to-advance-applied-research-in-cybersecurity-to-support-national-defense). 22.01.2021).***

***

«Президент США Дональд Трамп в ночь перед уходом с должности подписал исполнительный указ, предписывающий провайдерам облачных услуг собирать «более полные данные» о своих иностранных клиентах.

Как пишет D-Russia со ссылкой на FCW, для проведения мероприятий, включающих «вредоносную кибердеятельность», иностранные субъекты используют американскую облачную инфраструктуру, что «чрезвычайно усложняет» отслеживание их действий, т.к. злоумышленники легко переходят в другое «облако», уничтожая свои следы. Иностранные же реселлеры американских IaaS-продуктов делают доступ к облачным сервисам ещё проще, что позволяет злоумышленникам избегать обнаружения, говорится в письме Трампа к Конгрессу.

Чтобы разобраться с этими угрозами, правительство должно потребовать у провайдеров «облаков» собирать и хранить более полные записи об иностранных клиентах, а также, возможно, ограничивать доступ к своим услугам для «определённых иностранных субъектов».

Каким именно иностранным клиентам можно будет «перекрывать воздух», смогут решать министры торговли, финансов, обороны, внутренней безопасности, глава госдепартамента, генпрокурор и начальник разведывательной службы.

Эксперты по кибербезопасности отмечают, что меры, предусмотренные указом, могут помочь правительству собрать больше данных, актуальных в свете недавнего киберпроникновения в сети американского правительства и крупных корпораций.

США должны перестать изображать жертву взлома – ветеран американской разведки

Хакеры, ответственные за этот взлом, как раз использовали американскую облачную инфраструктуру, что усложнило их обнаружение. Правда, новые требования могут стать проблемой для небольших провайдеров, которые понесут значительные расходы и, возможно, потеряют иностранных заказчиков.

Процедура введения в действие исполнительных указов президента США предусматривает полгода их обсуждения, и неизвестно, утвердит ли указ Трампа новый президент Джо Байден». ***(Последний указ Трампа посвящен «иностранным киберугрозам» // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5715546-Poslednij-ukaz-Trampa-posvyashhyon.html). 22.01.2021).***

***

«16 декабря 2020 года ЕС опубликовал предлагаемые изменения к существующей Директиве 2016/1148 о безопасности сетей и информационных систем (NIS2).

Предложения, которые были объявлены ключевым компонентом новой Стратегии кибербезопасности ЕС, предназначены для развития и отмены существующей структуры НИС. Они включают в себя ряд значительных изменений, вносимых в существующий режим, включая расширение сферы применения закона на дополнительные отрасли промышленности, усиление существующих правил в отношении требований безопасности и отчетности об инцидентах, а также увеличение максимальных штрафов, которые могут применяться.

NIS2 появился чуть более чем через два года после того, как первоначальная Директива NIS 2016/1148 («NIS1») должна была вступить в силу во всех странах-членах ЕС. Он был введен для того, чтобы отреагировать на различные критические замечания и проблемы, связанные с NIS1, и отразить все более широкую цифровизацию европейской экономики, которая еще больше ускорилась во время пандемии COVID-19.

Ключевые изменения существующего режима

Хотя основная цель NIS2 остается прежней, предлагаются различные заметные изменения, которые могут существенно повлиять на организации в будущем, в том числе:

Введены новые отрасли

Ряд дополнительных секторов промышленности попадут в сферу действия NIS2 как часть нового определения «важных предприятий». К ним относятся цифровые провайдеры (социальные сети, торговые площадки и поисковые системы), фармацевтические компании, производители медицинского и электронного оборудования и курьерские службы.

Удалено различие между операторами основных услуг и поставщиками цифровых услуг

Прежнее различие между «операторами основных услуг» и «поставщиками цифровых услуг» будет устранено и объединено в единую категорию «существенных субъектов», которые будут подлежать самым строгим стандартам надзора. Соответствующие секторы, которые подпадают под эту категорию, включают финансовые услуги, энергетику, транспорт и цифровую инфраструктуру (например, поставщиков облачных услуг и центры обработки данных).

Требования к уведомлению о нарушениях за 24 часа

Обязательство согласно NIS1 незамедлительно уведомлять об инцидентах безопасности было значительно усилено. Организации, которые считаются существенными или важными, теперь должны будут предоставить первоначальное уведомление как соответствующему органу, так и затронутым пользователям, в течение 24 часов после того, как им станет известно об инциденте безопасности, который оказывает значительное влияние на предоставление услуг.

Улучшенное управление рисками и меры безопасности

Обязательства по информационной безопасности были усилены за счет введения специальных требований. Ожидается, что как важные, так и важные организации будут иметь в наличии различные меры, такие как анализ рисков и политики информационной безопасности, планы реагирования на инциденты, обеспечение непрерывности бизнеса и кризисное управление, а также надежные процессы управления киберрисками в цепочке поставок.

Управление со стороны высшего руководства

Старшее руководство возьмет на себя дополнительные обязанности по утверждению адекватности упомянутых выше мер по управлению рисками и безопасности. Это будет включать как надзор за внедрением соответствующих стандартов безопасности, так и ответственность за их несоблюдение.

Усиленный надзор и контроль

Государства-члены должны будут предоставить своему соответствующему компетентному органу особые полномочия, включая право налагать штрафы в размере до 10 миллионов евро или 2% от годового мирового оборота (в зависимости от того, что является самым высоким) за наиболее серьезные нарушения. Важнейшие организации будут подвергаться проактивному надзору («ex ante»), который должен включать возможность проведения выборочных проверок и сканирований безопасности систем организации на предмет уязвимости. Для сравнения, важные субъекты будут подлежать ответному исполнению («постфактум») только в том случае, если о нарушении станет известно компетентным органом. Однако будет применяться тот же уровень штрафов, и аудит может быть проведен.

Внедрение NIS2 будет происходить параллельно с новой предложенной директивой, касающейся устойчивости критически важных объектов в таких секторах, как энергетика и транспорт. Это также является частью того же пакета мер, объявленных в рамках новой стратегии кибербезопасности ЕС. Директива потребует от государств-членов идентифицировать критически важные организации, которые действуют в пределах их юрисдикции, и налагает на такие организации дополнительные обязательства, выходящие за рамки NIS2, такие как принятие соответствующих технических и организационных мер для обеспечения устойчивости их операций.

Следующие шаги

Предложение NIS2 теперь будет предметом переговоров между Советом ЕС и Европейским парламентом. После публикации окончательной версии государствам-членам будет предоставлено 18 месяцев для преобразования Директивы в национальное законодательство». ***(Eduardo Ustaran, Dan Whitehead. EU seeks to bolster cybersecurity regulation with the introduction of NIS 2.0 // Hogan Lovells (https://www.engage.hoganlovells.com/knowledgeservices/viewContent.action?key=Ec8teaJ9Var2ArxFHqAN18xgHJMKLFEppVpbbVX%2B3OXcP3PYxlq7sZUjdbSm5FIetvAtgf1eVU8%3D&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQ0qFfoEM4UR4%3D&emailtofriendview=true&freeviewlink=true). 06.01.2021).***

***

«Согласно Государственному контролю, многомиллиардное превышение бюджета Министерства обороны было вызвано отчасти из-за того, что оно тратит деньги на новые яркие "кибер-возможности".

Минобороны столкнулось с «недоступным» планом расходов до 2030 года из-за плохого управления и планирования, говорится в последнем отчете НАО.

«Департамент сталкивается с фундаментальной проблемой, заключающейся в том, что его амбиции намного превышают имеющиеся ресурсы», - гремел он. «В результате краткосрочный подход к финансовому менеджменту привел к увеличению ценового давления, которое не позволяло бюджетам высшего уровня развивать военный потенциал таким образом, чтобы обеспечить соотношение цены и качества».

Министерство обороны столкнулось с бюджетной черной дырой, измеряемой миллиардами, благодаря своей расточительности - и даже объявления о пополнении денежных средств в размере 4 млрд фунтов стерлингов в год в период с настоящего момента до 2024 года в дополнение к его годовому бюджету в размере 41,2 млрд фунтов стерлингов будет недостаточно. чтобы подключить его, по мнению аудиторов.

Представители Министерства обороны сумели потратить, по словам NAO, «2,1 млрд фунтов дополнительных затрат на программу оснащения Стратегического командования, что отражает 1,1 млрд фунтов новых инвестиций для заполнения пробелов в возможностях». Вдобавок к этому, желание Минобороны «усилить киберпотенциал» в сочетании с планами по расширению «глобальной связи» привело к «росту затрат на 1,1 млрд фунтов стерлингов».

Как было объявлено в ноябре, подпиткой этой кибер-управляемой бюджетной недержания стало создание Национальной киберсилы (NCF). Хотя бюджет этого года включал 141 миллион фунтов стерлингов на «риски критического потенциала», включая NCF, Минобороны по-прежнему настаивало на том, что «потребуется дополнительное финансирование для развития военного потенциала, такого как его кибер-устойчивость».

Этот акцент на «киберпространстве», невзирая на бюджетные ограничения, даже заставил некоторых хитрых армейских офицеров предложить сократить танки в пользу киберполков, что, возможно, было насмешкой или политическим шагом для защиты дряхлых британских подразделений тяжелых танков от бобовых атак ручка.

В то время как высшее руководство все более и более разумно сосредотачивается на возрастающих цифровых угрозах, исходящих от России и Китая, кажется, что их ответы начинаются и заканчиваются словами «бросьте нам больше денег».

Остальная часть отчета была посвящена тому, насколько оборудование американского производства, входящее в портфель основных проектов Министерства обороны, является жерновом на финансовой шее министерства.

«Четвертый год подряд, - вздыхает NAO в своем отчете, - план оборудования остается недоступным по цене. Однако Департамент до сих пор не создал надежной основы для оценки доступности проектов по оборудованию, а также своей оценки нехватки финансирования в План на 2020-2030 годы, вероятно, будет

недооценивать растущее финансовое давление, с которым он сталкивается». ***(Gareth Corfield. Ministry of Defence's cyber warfare drive is helping burn a hole through its budget, warns UK's National Audit Office // The Register(https://www.theregister.com/2021/01/14/nao_ministry_defence_budget_report_cyber/). 14.01.2021).***

***

Російська Федерація та країни ЄАЕС

«В четверг вечером правительство России выпустило предупреждение о возможных кибератаках со стороны США в ответ на инцидент с SolarWinds.

Ответ российского правительства последовал после комментариев, сделанных новой администрацией Байдена ранее в тот же день.

Ответ Москвы на этот комментарий пришел через несколько часов в виде бюллетеня по безопасности, опубликованного Национальным координационным центром компьютерных инцидентов (НКЦКИ), агентством безопасности, основанным Федеральной службой безопасности (ФСБ), службой внутренней безопасности и разведки России.

В кратком заявлении цитируются комментарии администрации Байдена, интерпретированные как угрозы, и приводится список из 15 передовых методов безопасности, которых предприятиям следует придерживаться, чтобы оставаться в безопасности в Интернете.

Лучшие практики, включенные в предупреждение, основаны на стандартных рекомендациях по безопасности и ничего, о чем компании или даже самый низкоквалифицированный специалист по безопасности еще не знали.

Предупреждение системы безопасности было опубликовано скорее как ответ на агрессивные заявления администрации Байдена ранее в тот же день.

Комментарии Белого дома повторяют тон, заданный две недели назад, когда официальные лица США из ФБР, CISA, ODNI и NSA официально обвинили Россию в организации широкомасштабной атаки на цепочку поставок SolarWinds.

Кремлевские официальные лица неоднократно отрицали свою причастность к инциденту с SolarWinds.

Во время вчерашней пресс-конференции администрация Байдена также пообещала выделить 9 миллиардов долларов на кибербезопасность после взлома SolarWinds». ***(Catalin Cimpanu. FSB warns of US cyberattacks after Biden administration comments // ZDNet (https://www.zdnet.com/article/fsb-warns-of-us-cyberattacks-after-biden-administration-comments/). 22.01.2021).***

***

«Российский Национальный координационный центр по компьютерным инцидентам (НКЦКИ) предупредил о возможности проведения США и их союзниками кибератак на объекты критической информационной инфраструктуры России. Об этом говорится в бюллетене центра, опубликованном 21 января.

«В условиях постоянных обвинений в причастности к организации компьютерных атак, высказываемых в адрес Российской Федерации представителями США и их союзниками, а также звучащих с их стороны угроз проведения «ответных» атак на объекты критической информационной инфраструктуры Российской Федерации, рекомендуем принять <…> меры по повышению защищенности информационных ресурсов», — отмечается в документе.

Так, по предписанию НКЦКИ, организациям необходимо привести в актуальное состояние планы, инструкции и руководства по реагированию на компьютерные инциденты. Также в рекомендациях говорится, что стоит предупредить сотрудников о вероятных фишинговых атаках, провести аудит сетевых средств защиты информации и антивирусов, избегать использования сторонних DNS-серверов.

Помимо этого, лучше обновить пароли всех пользователей, обеспечить антивирусом анализ входящей и исходящей электронной почты, проводить мониторинг безопасности систем «с повышенной бдительностью», а также следить за наличием необходимых обновлений безопасности ПО.

В конце декабря 2020 года стало известно о том, что советники Джо Байдена — нынешнего президента США — обсуждают возможность введения санкций против России в связи с кибератакой в отношении американских правительственных учреждений, причастность к которой в Вашингтоне приписывают Москве…

В тот же день пресс-секретарь президента РФ Дмитрий Песков заявил, что Россия не имеет отношения к хакерским атакам на американские госучреждения. Представитель Кремля призвал прекратить голословные обвинения в адрес РФ». ***(Центр кибербезопасности РФ предупредил об угрозе атак со стороны США // Газета «Известия» (https://iz.ru/1114817/2021-01-22/tcentr-kiberbezopasnosti-rf-predupredil-ob-ugroze-atak-so-storony-ssha). 22.01.2021).***

***

«Госдума в среду приняла в первом чтении правительственный законопроект о введении административных штрафов до 500 тыс. рублей за нарушение требований по обеспечению безопасности критической информационной инфраструктуры РФ, а также за несвоевременное предоставление сведений органам, отвечающим за ликвидацию компьютерных атак.

Согласно изменениям, вносимым в Кодекс об административных правонарушениях, нарушение требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры, обеспечению их работы и безопасности в рамках действующих законов и регламентов повлечет наложение штрафа на должностных лиц в размере от 10 тыс. до 50 тыс. рублей, а на юридических лиц - от 50 тыс. до 100 тыс. рублей.

Нарушение "порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак", согласно тексту законопроекта, будет грозить должностным лицам штрафом

в размере от 10 тыс. до 50 тыс. рублей, а юридическим лицам - от 100 тыс. до 500 тыс. рублей. Также за нарушение порядка обмена данными об инцидентах между субъектами такой инфраструктуры, иностранными уполномоченными органами, международными организациями и НПО, работающими в сфере реагирования на киберугрозы, предусмотрены штрафы для должностных лиц - от 20 тыс. до 50 тыс. рублей, для юридических лиц - от 100 тыс. до 500 тыс. рублей.

Если в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы не были предоставлены или же несвоевременно, с нарушением сроков, поступили данные, предусмотренные законодательством в области обеспечения безопасности критической информационной инфраструктуры, штраф для должностных лиц составит от 10 тыс. до 50 тыс. рублей, а для юридических лиц - от 100 тыс. до 500 тыс. рублей.

Если уполномоченный орган исполнительной власти не будет уведомлен (уведомлен с опозданием) о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости, то штраф составит от 10 тыс. до 50 тыс. рублей для должностных лиц и от 50 тыс. до 100 тыс. рублей - для юридических лиц. Согласно пояснительной записке, "размеры предлагаемых штрафов учитывают размер средней заработной платы руководителей структурных подразделений по обеспечению информационной безопасности». ***(Дума одобрила введение штрафов за нарушения при защите критической IT-инфраструктуры // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5716475-Duma-odobrila-vvedenie-shtrafov.html). 28.01.2021).***

***

«Российская Федерация видит определенные сигналы новой администрации США для налаживания серьезного диалога с Москвой по вопросам сотрудничества в киберсфере, заявил 26 января директор департамента международной информационной безопасности МИД России Андрей Крутских.

По его словам, наблюдаются признаки заинтересованности Вашингтона в налаживании серьезного разговора с Москвой.

«Я думаю, что сфера киберсотрудничества или, по крайней мере, наращивания взаимопонимания с США — одна из приоритетных не только для нас, но если отбросить всю американскую идеологию, то и для Вашингтона», — цитирует дипломата «РИА Новости»…». ***(МИД сообщил о заинтересованности США в сотрудничестве в киберсфере // Газета «Известия» (https://iz.ru/1116452/2021-01-26/mid-soobshchil-o-zainteresovannosti-ssha-v-sotrudnichestve-v-kibersfere). 26.01.2021).***

***

«7 января 2021 года Австралийский центр кибербезопасности (ACSC) выпустил обновленное руководство по управлению рисками цепочки киберпоставок и выявлению рисков цепочки поставок в киберпространстве, чтобы помочь предприятиям выявлять киберриски, связанные с использованием поставщиков, производителей, дистрибьюторов и розничных продавцов, и управлять ими.

В обновленном руководстве по управлению рисками цепочки поставок в киберпространстве изложены основные шаги, которые следует предпринять предприятиям, чтобы:

- определить участников цепочки поставок в киберпространстве;
- понимать соответствующие риски цепочки поставок;
- установить соответствующие ожидания кибербезопасности для различных участников;
- аудит участников цепочки поставок на соответствие; и
- отслеживать и улучшать свои методы кибербезопасности цепочки поставок на итерационной основе.
- Обновленное руководство по выявлению рисков в цепочке поставок в киберпространстве рассматривает конкретные риски, которые могут возникнуть в цепочке поставок из-за:
- иностранный контроль, влияние или вмешательство в отношении участников цепочки поставок;
- плохая практика безопасности участников цепочки поставок;
- непрозрачность участников; и
- объем доступа и привилегий для соответствующих продуктов и услуг.

Рекомендации по аутсорсингу, содержащиеся в Руководстве по информационной безопасности правительства Австралии (ISM), также могут быть интересны любому бизнесу, который рассматривает или находится в процессе привлечения участников цепочки поставок или осуществления любой формы аутсорсинговой деятельности». ***(Jarrod Bayliss-McCulloch. ACSC updates guidance on cyber risks in the supply chain // Baker McKenzie (https://viewpoints.bakermckenzie.com/post/102gond/acsc-updates-guidance-on-cyber-risks-in-the-supply-chain). 14.01.2021).***

***

Протидія зовнішній кібернетичній агресії

«Федеральное бюро расследований США начало расследование после того, как на домашний адрес главы компании FireEye Кевина Мандиа была отправлена открытка с карикатурой и словами «Эй, смотрите, русские» и «Путин сделал это!». Таким образом хакеры, предположительно решили

поставить под сомнение способность компании связать кибератаки с правительством России.

Открытка поступила через несколько дней после того, как специалисты выявили масштабную кибератаку на федеральные ведомства и компании США. Как сообщает информагентство Reuters, на момент получения открытки в FireEye не подозревали, кто может быть ответственным за атаку. ФБР, Агентство по кибербезопасности и обеспечению защиты инфраструктуры США (CISA) и Разведывательное сообщество США (ODNI) позже допустили причастность России к хакерской атаке на американские федеральные ведомства.

Примечательно, что исследователь в области дезинформации Тодд Хелмус (Todd Helmus) из Rand Corporation получил аналогичную открытку в 2019 году. Хельмус сказал, что получил открытку после того, как дал в Конгрессе показания о российской тактике дезинформации». ***(Глава FireEye получил открытку с карикатурой после обнаружения атаки на ведомства США // SecurityLab.ru (https://www.securitylab.ru/news/515402.php). 12.01.2021).***

***

«В начале 2020 года мощная DDoS-атака оставила без интернета и связи - почти на семь часов - пользователей в Иране. Кроме сайта госуслуг, пострадали два популярных мобильных оператора. Иран обвинил в инциденте США, расценив кибератаку как ответную реакцию на ракетный обстрел американских баз в Ираке. В современном мире максимальный социальный и экономический ущерб может быть нанесен за счет отключения пользователей и бизнеса от связи и интернета. Мы уже привыкли быть на связи 24/7, тем более когда в условиях пандемии компании массово перевели сотрудников на дистанционный формат работы. Злоумышленники, получившие доступ к инфраструктуре телеком-компаний, могут не только завладеть персональной и финансовой информацией пользователей, но и оставить город, регион, а то и целую страну без связи.

Политический след

В целом значительная часть атак на телекоммуникационный сектор связана с разворачивающимися сегодня кибервойнами и затрагивает интересы целых государств. Согласно свежему отчету Hi-Tech Trends 2020-2021, представленному Group-IB на международной конференции CyberCrimeCon2020, прогосударственные группировки проявляют к телеком-сектору особый интерес, реализуя изощренные атаки. За анализируемый период в телекоммуникационном секторе проявляли активность шесть групп, связанных со спецслужбами. Из числа подобных групп сегмент телекома в этом году атаковали Winnti и Mikroceen (Китай), OilRig (Иран), Molerats (арабское происхождение) с целью шпионажа и диверсии.

В первую очередь свои возможности по шпионажу за операторами мобильной связи наращивает Китай. Для этого Winnti разработала специальный троян для Linux-серверов, который позволяет перехватывать SMS по определенным критериям. С помощью вредоносной программы группа в 2020 году

получила доступ к сообщениям лиц, представляющих интерес для китайского правительства.

Вызовы времени

Основными угрозами для телеком-сектора в этом году является BGP-Hijacking (незаконный захват/утечка пулов IP-адресов путем повреждения таблиц маршрутизации интернета, которые поддерживаются с помощью протокола пограничного шлюза BGP) и DDOS-атаки, следует из Hi-Tech Trends.

Протокол BGP позволяет выполнить соединения самым быстрым и эффективным путем, но имеет серьезное допущение: предполагается, что AS сообщают корректную информацию о тех IP-префиксах, которые им принадлежат. Если злоумышленник получает контроль над роутером, стоящим на границе такой автономной системы и анонсирующим префиксы, он может исказить маршрутизацию. В результате трафик пользователей, работающих с определенным сайтом, пойдет через оборудование преступников. Преступники могут использовать это для шпионажа, кражи данных банковских карт, другой личной информации для шантажа и вымогательства.

Group-IB в 2020 году зафиксировала девять случаев BGP-Hijacking. Самыми крупными инцидентами стали компрометация 90 тыс. префиксов AS205310 (AS - автономная система) Beiersdorf Shared Services GmbH в Германии (маршруты были перенаправлены в AS15943 вместо AS8220) и утечка 9328 префиксов из 1250 AS (включая Akamai, Cloudflare, Vodafone, NTT, Amazon, NVIDIA) в Бразилии (AS263444 Open X Tecnologia Ltda).

Наибольшее количество DDOS-атак, по данным Group-IB, пришлось на первую половину 2020 года, и именно тогда произошел наиболее масштабный инцидент в отрасли. Согласно отчету Amazon за I квартал 2020 года, служба AWS Shield в середине февраля отразила самую крупную DDoS-атаку из когда-либо зафиксированных, объем которой достигал 2,3 Тб/с. Она проведена с использованием взломанных CLDAP веб-серверов и продолжалась в течение трех дней. CLDAP (Connectionless Lightweight Directory Access Protocol) - это альтернатива более старому LDAP, который злоумышленники используют с 2016 года. С помощью CLDAP-сервера они способны отразить и приумножить DDoS-трафик в 76 раз от его первоначального объема. Предыдущий рекорд - 1,7 Тб/с - зафиксирован в марте 2018 года.

21 июня 2020 года Akamai сообщила об атаке на европейскую финансовую организацию объемом 809 млн пакетов в секунду (MPPS). Важная особенность - подавляющее большинство трафика атаки (96,2%) получено от IP-адресов, которые не зарегистрированы в предыдущих атаках 2020 года, что указывает на появление новой бот-сети. Это нападение примечательно не только своими размерами, но и скоростью, с которой оно достигло своего пика, - примерно за две минуты. В общей сложности сбой продолжался чуть менее 10 минут.

Еще одной угрозой для телекома являются проблемы, связанные с распространением сетей 5G. Их стандартизация завершится в ближайшее время. Более того, сейчас идет активная конкурентная борьба не только между технологическими гигантами, но и между странами (лидируют США и Китай). Выгода очевидна: возможность заставить весь рынок играть по своим правилам.

Вполне естественно, что эта тема вызывает интерес киберпреступников, поскольку дает доступ к большой аудитории. В отличие от предыдущих стандартов связи, технологии пятого поколения используют программные платформы для реализации сверхскоростного подключения. Это означает, что все угрозы для серверных и программных решений становятся актуальными для операторов 5G. Среди них атаки APT-групп, связанные с BIOS/UEFI, side channel и supply chain, для шпионажа и саботажа. Также благодаря большому количеству подключенных устройств и широкой полосе пропуска может значительно увеличиться масштаб DDoS-атак.

Недооцененный риск

Учитывая нарастающие противостояния между государствами, Group-IB ожидает, что вскоре появятся первые атаки на операторов сотовой связи. Они вызовут логические перезагрузки сети, что приведет к каскадному эффекту и повлияет на множество секторов экономики. Также в связи с продолжающимся переходом сотрудников на удаленку (status quo может сохраниться и после пандемии) количество атак на роутеры и системы хранения данных возрастет: они помогают прогосударственным хакерам более эффективно получать доступ к корпоративным сведениям, не проникая в периметр организации. Нельзя сбрасывать со счетов атаки с помощью социальной инженерии. К сожалению, человеческий фактор - одно из наиболее слабых мест в корпоративной системе информационной безопасности.

Для решения проблем сложных угроз телекоммуникационные компании вынуждены постоянно адаптировать и видоизменять свои стратегии - в частности, организовать комплексные системы безопасности, которые обеспечивают закрытие не только внешнего периметра от атак извне, направленных на канальную часть или на уровень веб-приложений, но и отслеживание проблем внутри инфраструктуры оператора.

Для защиты от DDoS-атак Group-IB рекомендует перейти на использование внешнего балансировщика или проксирующего сервиса, усложнять архитектуру, переносить IP-адреса на внешние сервисы. Также необходимо увеличивать полосы пропускания, закупать аппаратные средства фильтрации, переходить на операторов с соответствующими anti-DDoS-мощностями. Чтобы противостоять BGP-Hijacking, нужно повышать общую осознанность среди других участников в сети, выработать цифровой аналог "группового иммунитета" - иметь как можно больше "стыков" с другими провайдерами. Вторая мера - наблюдать за своими сетевыми префиксами в других AS, в случае ошибочного анонса префикса или обнаружения нападения срочно связываться с RIR (региональная регистратура интернета), которые допускают транзитную передачу ложного префикса для пресечения подобной активности.

Впрочем, только этими мерами защиты не обойтись. На CyberCrimeCon2020 Group-IB представила два новых класса решений - Threat Intelligence & Attribution (TI&A) и Threat Hunting Framework. TI&A гибко формирует карту угроз под конкретную компанию, динамически выстраивая связи между разрозненными событиями, и атрибутирует атаку до конкретной хакерской группы. Появление на рынке TI&A знаменует собой открытие нового класса решений для сбора данных

об угрозах и атакующих, релевантных для конкретной организации, с целью исследования, проактивной охоты за хакерами и защиты сетевой инфраструктуры. THF предназначена для защиты ИТ и технологических сетей от неизвестных ранее угроз и целевых нападений, поиска угроз как внутри, так и вне сети, а также расследования инцидентов кибербезопасности и немедленного реагирования на них в целях минимизации последствий». ***(Станислав Фесенко. Вне зоны доступа: актуальные киберугрозы для телеком-отрасли // ComNews (https://www.comnews.ru/content/212399/2021-01-11/2021-w02/vne-zony-dostupa-aktualnye-kiberugrozy-dlya-telekom-otrasli). 11.01.2021).***

***

«Джон Филдинг, управляющий директор, EMEA Apricorn, объясняет, что необходимо сделать организациям государственного сектора, чтобы избежать утечек и потерь за счет надлежащей защиты данных и устройств.

Правительство окутано конфиденциальностью, но сохранение конфиденциальности частной информации становится все более сложной задачей для государственного сектора. Помимо государственной тайны, государственные ведомства хранят огромное количество данных о своих гражданах, и все они очень ценны как для владельца, так и для любого злоумышленника, желающего извлечь выгоду из того, что они заполучили его.

В то время как правительственные ведомства постоянно стремятся улучшить безопасность своих данных, самый большой риск, как правило, исходит от инсайдера, из-за случайной потери и кражи устройств, что может привести к утечке данных.

Количество сообщений о нарушениях растет

Фактически, Apricorn объявил о результатах (октябрь 2020 г.) запросов о свободе информации (FoI) и данных из годовых отчетов 17 государственных органов. Ответы показали, что правительственные ведомства сообщили о тысячах утечек личных данных с многочисленными уведомлениями в ICO в период с 2019 по 2020 год.

Например, в годовом отчете и отчетности Агентства по лицензированию водителей и транспортных средств (DVLA) за 2019–2020 годы было представлено 181 уведомление в Управление комиссара по информации (ICO) только за последний год. Кроме того, запросы FoI, представленные в Паспортный стол НМ (HMPO), показали, что с 1 августа 2019 года по 31 июля 2020 года Управление офицера по защите данных (DPO) получило 1291 отчет об инцидентах с данными в отношении HMPO, 1280 из которых были оценены как личные. Утечки данных.

Эти отделы имеют дело с тысячами, даже миллионами записей, содержащих личные данные или конфиденциальную информацию. Независимо от того, являются ли это незначительные нарушения, не требующие дальнейших действий, ясно, что необходимо сделать больше, и отделам необходимо рассмотреть инструменты, необходимые для снижения этих показателей.

Согласно Годовому отчету ICO за 2019-2020 годы, в ICO в 2019-2020 годах было сообщено о 11854 утечках персональных данных, и это касается только тех, которые требуют уведомления. Например, в годовом отчете службы безопасности

Министерства внутренних дел отмечается, что в 2019-2020 годах было зарегистрировано 4204 инцидента, но только 25 были выделены как особо серьезные, что означает необходимость уведомления ICO.

При таком большом количестве нарушений со стороны правительства необходимо сделать больше для обеспечения безопасности его данных. Существует острая необходимость оцифровки во всем секторе для повышения эффективности рабочих процессов и процессов, которые включают хранение, управление и резервное копирование информации. Текущий уровень безопасности недостаточен для безопасной поддержки новых цифровых способов работы, особенно когда такое количество сотрудников получает удаленный доступ к системам, сетям и приложениям.

Основное шифрование

Для государственных ведомств, отвечающих за конфиденциальные данные и интеллектуальную собственность бесчисленных налогоплательщиков, одобренные корпорациями устройства хранения с аппаратным шифрованием должны быть стандартными. Шифрование необходимо, чтобы гарантировать, что данные на них будут недоступны, если эти устройства будут потеряны, украдены или забыты, если они попадут в чужие руки. Компании должны принять необходимость оцифровки и преимущества, которые она дает для хранения документов, резервного копирования в Интернете, управления документами и удаленной работы. Этот процесс быстрее, эффективнее и, в конечном итоге, безопаснее, чем автономные эквиваленты, с соответствующими элементами управления.

Шифрование часто может быть ограничено другими методами обеспечения безопасности, и хотя многие компании сейчас шифруют данные, хранящиеся на мобильных устройствах и съемных устройствах хранения, исследование Apricorn в начале 2020 года по внедрению технологии шифрования в организациях показало, что многие компании не имеют в дальнейшем планирует расширить шифрование USB-накопителей (38%), ноутбуков (32%), настольных компьютеров (37%), мобильных телефонов (31%) и портативных жестких дисков (40%).

Государственные учреждения должны иметь видимость всех устройств, имеющих доступ к сети. Политики безопасности, которые диктуют, какое оборудование могут использовать сотрудники, могут быть сложными для обеспечения соблюдения и могут снизить производительность, и, хотя меры безопасности, такие как брандмауэры, необходимы, они не защищают сотрудников от неправильного использования или потери устройств.

Аппаратное шифрование обеспечивает гораздо большую безопасность, чем программное шифрование, а USB-устройства хранения с аппаратным шифрованием и аутентификацией с помощью PIN-кода предлагают дополнительные существенные преимущества. Отсутствие программного обеспечения исключает риск кейлоггеров и не ограничивает использование определенных операционных систем; все процессы аутентификации и шифрования происходят внутри самого устройства, поэтому пароли и ключевые данные никогда не передаются на главный компьютер.

Развертывая съемные устройства хранения со встроенным аппаратным шифрованием, правительственные ведомства могут развернуть это по всей

организации, гарантируя, что все данные можно безопасно хранить или перемещать в автономном режиме. Даже если устройство будет потеряно или украдено, информация будет недоступна для всех, кто не имеет к ней доступа.

Шифрование специально рекомендуется в статье 32 GDPR для защиты личных данных, а также в статье 34, в которой подробно описывается сокращение обязательств для тех, кто пострадал от взлома, когда данные, о которых идет речь, зашифрованы. Государственные органы должны серьезно относиться к шифрованию, и данные должны быть зашифрованы как стандарт. Шифрование - ключевой компонент в «комплекте» соответствия, не только снижающий вероятность нарушения, но и смягчающий потенциальные финансовые санкции. Государственные департаменты должны исследовать, идентифицировать и санкционировать эти зашифрованные устройства, чтобы избежать риска взлома и штрафов за несоблюдение.

Осведомленность сотрудников

Помимо этого, необходимо обучать сотрудников передовым методам обеспечения безопасности, чтобы гарантировать, что они следуют необходимым политикам и не подвергают данные без необходимости риску. Образование сотрудников было выделено в недавнем опросе Apricorn более 30% респондентов как самая большая область, в которой компаниям необходимо вносить изменения для повышения кибербезопасности. Органы государственного сектора должны обеспечивать соблюдение элементарной гигиены безопасности и должны отслеживать, как данные обрабатываются, хранятся, извлекаются и удаляются, чтобы исправить любые недостатки.

Образование играет решающую роль в обеспечении безопасности данных, и сотрудники должны быть оснащены технологиями и процессами для защиты своих активов. Данные должны быть зашифрованы, пароли должны быть защищены, а правила должны быть введены и соблюдены, чтобы ограничивать и ограничивать доступ сотрудников только к тем системам, которые необходимы, а не открывать доступ ко всей сети.

Исследование FoI также показало, что некоторые правительственные ведомства не могут легко и эффективно получить доступ к информации об утечках данных. Соответствующие департаменты должны более эффективно управлять этим процессом, чтобы информация о местонахождении данных и о том, подвергались ли они риску, была хорошо задокументирована, а информация, хранящаяся в центральной базе данных, была легко доступна уполномоченным лицам и не требовала многократного дней на восстановление.

Если правительственные ведомства хотят навести порядок в безопасности своих данных, шифрование должно быть во главу угла их стратегии, чтобы гарантировать безопасность данных, где бы они ни находились». ***(Why lack of encryption is putting public data at risk // Open Access Government (https://www.openaccessgovernment.org/why-lack-of-encryption-is-putting-public-data-at-risk/101928/). 20.01.2021).***

***

«В пятницу агентство Reuters сообщило, что президент Джо Байден нанимает больше экспертов по кибербезопасности, поскольку США все глубже разбирается во взломе SolarWinds в 2020 году. Спецслужбы США приписывают массовый взлом России.

Президент создаст новый офис, ориентированный на кибербезопасность, во главе с национальным кибердиректором в соответствии с недавним законом. По данным Reuters, Джен Истерли, которая была специальным помощником президента Барака Обамы и старшим директором по борьбе с терроризмом Совета национальной безопасности, является ведущим кандидатом на роль кибердиректора. В настоящее время она возглавляет отдел устойчивости инвестиционного банка Morgan Stanley.

Во вторник, в свой последний полный рабочий день в должности, бывший президент Дональд Трамп подписал указ, призванный воспрепятствовать иностранным игрокам использовать платформы облачных вычислений для вмешательства в дела США.

В ноябре Трамп уволил директора Агентства по кибербезопасности и безопасности инфраструктуры Криса Кребса после того, как агентство опровергло утверждения о фальсификации выборов. С тех пор SolarWinds наняла Кребса для консультации по поводу массового взлома. Байден намерен назначить Роба Силверса, который был помощником секретаря администрации Обамы по киберполитике в Министерстве внутренней безопасности, на роль Кребса, сообщает Reuters.

Ни Morgan Stanley, ни Silvers, ни Белый дом не сразу ответили на запросы о комментариях». ***(Sean Keane. Biden reportedly hiring cybersecurity experts in wake of SolarWinds hack // CNET (https://www.cnet.com/news/biden-reportedly-gathers-cybersecurity-experts-in-wake-of-solarwinds-hack/). 22.01.2021).***

***

Створення та функціонування кібервійськ

«Госсекретарь Майк Помпео одобрил создание в четверг Бюро безопасности киберпространства и новых технологий (CSET) в Государственном департаменте, которое возглавит дипломатические усилия по отражению кибератак со стороны зарубежных стран.

Согласно заявлению, цель CSET - «возглавить дипломатические усилия правительства США по широкому кругу вопросов безопасности международного киберпространства и возникающих вопросов технологической политики, которые влияют на внешнюю политику и национальную безопасность США». Департамент уведомил Конгресс о своем намерении создать CSET в июне 2019 года.

«Необходимость реорганизации и ресурсного обеспечения киберпространства Америки и дипломатии новой технологической безопасности посредством создания CSET является критической, поскольку вызовы национальной безопасности США, которые представляют Китай, Россия, Иран, Северная Корея и другие конкуренты и противники киберпространства и новых

технологий, увеличилась только после того, как в июне 2019 года Департамент уведомил Конгресс о своем намерении создать CSET», - говорится в заявлении.

Однако идея создать кибер-бюро при Госдепартаменте возникла еще раньше.

В январе 2019 года члены Палаты представителей внесли законопроект о создании Управления по международной политике в области киберпространства во главе с послом киберпространства.

Решение Помпео утвердить новое кибербюро позволит Департаменту продвинуться вперед в создании CSET и сотрудничать с партнерами и союзниками по насущным вопросам национальной безопасности». ***(GRACE DILLE. Pompeo Approves New Bureau of Cyberspace Security and Emerging Technologies // MeriTalk (https://www.meritalk.com/articles/pompeo-approves-new-bureau-of-cyberspace-security-and-emerging-technologies/). 08.01.2021).***

***

«Завдяки зусиллям НАТО у Молдові відкрито Центр з реагування на кібернетичні інциденти, який покликаний підвищити стійкість військових мереж та критичної інфраструктури до кібернетичних атак.

Таке повідомлення оприлюднене у четвер на сайті Північноатлантичного Альянсу.

«21 січня 2021 року за допомогою НАТО в Молдові був відкритий Центр з реагування на кібернетичні інциденти для збройних сил Молдови. Ці спроможності були створені за підтримки програми НАТО «Наука заради миру та безпеки» у співробітництві з Агентством НАТО з інформації та комунікації, за результатами реалізації багаторічного проєкту. Центр допоможе мінімізувати будь-які загрози, що пов’язані із кібернетичними інцидентами, забезпечити швидке та ефективне відновлення пошкодженого обладнання, а також запобігати подібним інцидентам у майбутньому», - йдеться у повідомленні.

Згаданий проєкт був розроблений для розв'язання проблем, що були визначені урядом Молдови в тісному співробітництві із технічними експертами НАТО. Він включає курс спеціалізованого тренування, яке головним призначенням має найбільш ефективне використання людського, технічного та кібернетичного потенціалу для протидії загрозам для військової комп’ютерної системи та для критичної інфраструктури.

Як зазначається, програма НАТО «Наука заради миру і безпеки», починаючи з 1995 року, дозволила реалізувати в Молдові кілька важливих проєктів, зокрема, у таких сферах як кібернетична безпека, захист від біологічних загроз, розвиток передових технологій, надала належне тренування та досвід багатьом молодих науковцям і експертам, підвищила їх здатність ефективно співпрацювати з партнерами у НАТО…». ***(НАТО допомогло створити Центр з реагування на кібернетичні інциденти в Молдові // Укрінформ (https://www.ukrinform.ua/rubric-world/3175708-nato-dopomoglo-stvoriti-centr-z-reaguvanna-na-kiberneticni-incidenti-v-moldovi.html). 22.01.2021).***

***

«Агентство по кибербезопасности и безопасности инфраструктуры (CISA) поздно вечером в пятницу выпустило новое предупреждение, связанное с российским взломом продуктов SolarWinds Orion, в котором CISA предупреждает, что обнаружило свидетельства активности повышенной постоянной угрозы (APT) после взлома в облачной среде.

В предупреждении говорится, что CISA «видел, как субъект APT использовал скомпрометированные приложения в среде Microsoft 365 (M365) / Azure жертвы и использовал дополнительные учетные данные и доступ через интерфейс прикладного программирования (API) к облачным ресурсам организаций частного и государственного сектора».

По словам агентства, деятельность, отмеченная CISA, является дополнением к тому, что было описано ранее в предупреждении 17 декабря, выпущенном вскоре после того, как взлом SolarWinds стал достоянием общественности.

В ответ на сегодняшнее предупреждение CISA выпустила новые ресурсы для описания APT-активности и рекомендаций по инструментам исправления с открытым исходным кодом.

«Защитники сети могут использовать эти инструменты, чтобы помочь обнаружить и устранить действия злонамеренных APT-агентов в рамках продолжающейся компрометации цепочки поставок», - заявило агентство, добавив, что «настоятельно рекомендует пользователям и администраторам» просмотреть свое предупреждение для получения дополнительной информации и контрмер обнаружения». ***(JOHN CURRAN. CISA Alert Flags Post-Hack APT Threat in Microsoft Cloud Environment // MeriTalk (https://www.meritalk.com/articles/cisa-alert-flags-post-hack-apt-threat-in-microsoft-cloud-environment/). 08.01.2021).***

***

«Судебная власть Соединенных Штатов объявила об аудите своих систем из-за опасений, что их файловая система с судебными делами была скомпрометирована.

Делая объявление, судебные органы заявили, что Административное управление судов США работает с Министерством внутренней безопасности над аудитом безопасности, касающимся уязвимостей в системе управления делами / электронных файлов дел (CM / ECF) судебной власти, которые серьезно рискуют подвергнуться серьезному риску. конфиденциальные закрытые документы, особенно запечатанные документы.

«Явное нарушение конфиденциальности системы CM / ECF из-за этих обнаруженных уязвимостей в настоящее время расследуется», - говорится в сообщении. «В связи с характером атак, анализ этого вопроса и его последствий продолжается».

Судебная власть сообщила, что в связи с продолжающимся расследованием федеральные суды по всей стране добавят новые процедуры безопасности, направленные на защиту конфиденциальных документов, поданных в суд.

В дальнейшем весьма конфиденциальные судебные документы, поданные в федеральные суды, будут приниматься для подачи в бумажной форме или с помощью «защищенного электронного устройства», такого как флэш-накопитель, и храниться в «защищенной автономной компьютерной системе». Документы не будут загружены в CM / ECF.

Документы, не считающиеся высокочувствительными, будут по-прежнему запечатываться в CM / ECF «по мере необходимости».

«Первоочередной задачей федеральной судебной власти должна быть честность и общественное доверие к работе и управлению ее судами», - сказал секретарь Судебной конференции Соединенных Штатов Джеймс К. Дафф.

Судебные органы заявили, что следуя указаниям Министерства внутренней безопасности, их суды приостановили любое национальное и местное использование продуктов SolarWinds Orion.

Ранее на этой неделе Министерство юстиции США (DOJ) подтвердило, что хакеры, стоящие за атакой цепочки поставок SolarWinds, нацелены на его ИТ-системы, где они увеличили доступ из троянизированного приложения SolarWinds Orion для перемещения по своей внутренней сети и доступа к учетным записям электронной почты некоторых своих сотрудников.

В настоящее время предполагается, что количество пострадавших сотрудников Министерства юстиции составляет от 3000 до 3450. Министерство юстиции заявило, что теперь блокировано вход злоумышленника.

В понедельник четыре агентства по кибербезопасности США опубликовали совместное заявление, в котором официально обвинили правительство России в организации атаки на цепочку поставок SolarWinds.

Официальные лица США заявили, что «серьезный постоянный злоумышленник, вероятно, российский по происхождению» был ответственен за взлом SolarWinds, который чиновники описали как «попытку сбора разведданных». ***(Asha Barbaschow. Investigation launched into vulnerabilities found within US Judiciary case file system // ZDNet (https://www.zdnet.com/article/investigation-launched-into-vulnerabilities-found-within-us-judiciary-case-file-system/). 08.01.2021).***

***

«Чешская компания по разработке программного обеспечения JetBrains опубликовала сегодня заявление, опровергающее сообщения New York Times и Wall Street Journal, в которых утверждается, что JetBrains находится под следствием на предмет возможного участия во взломе SolarWinds, затронувшем тысячи компаний по всему миру.

В отчетах со ссылкой на правительственные источники говорится, что официальные лица США рассматривают сценарий, когда российские хакеры взломают JetBrains, а затем предпримут атаки на ее клиентов, одной из которых была SolarWinds.

В частности, исследователи считают, что хакеры нацелены на продукт JetBrains под названием TeamCity, сервер CI / CD (непрерывная интеграция / непрерывная разработка), который используется для сборки компонентов в окончательное программное приложение в процессе, известном как «сборка».

Но в опубликованном сегодня сообщении в блоге генеральный директор JetBrains Максим Шафиров сказал, что чешская компания не знала, что в отношении нее ведется расследование в связи с ее участием в взломе SolarWinds.

«SolarWinds является одним из наших клиентов и использует TeamCity, систему непрерывной интеграции и развертывания, используемую как часть создания программного обеспечения», - сказал Шафиров.

«Компания SolarWinds не связалась с нами с какими-либо подробностями относительно взлома», - добавил он.

«Во-вторых, с нами не связывалось какое-либо правительство или агентство безопасности по этому поводу, и мы не знаем, что ведем какое-либо расследование. Если такое расследование будет проведено, власти могут рассчитывать на наше полное сотрудничество».

Однако генеральный директор JetBrains, гражданин России, не исключил полностью возможность того, что его продукт мог быть использован во взломе SolarWinds.

«Важно подчеркнуть, что TeamCity - это сложный продукт, требующий правильной настройки. Если TeamCity каким-то образом использовался в этом процессе, это вполне могло быть связано с неправильной настройкой, а не с конкретной уязвимостью», - сказал исполнительный директор.

Тем не менее, в двух отчетах также не очень ясно говорится о предполагаемом взломе JetBrains. Как ранее сегодня отметил в Твиттере Стефан Соэсанто, старший исследователь киберзащиты Центра исследований безопасности Швейцарского федерального технологического института (ETH) в Цюрихе, необходимо уточнить дополнительные детали, прежде чем обвинять JetBrains в какой-либо вине. взлом SolarWinds». ***(Catalin Cimpanu. JetBrains denies being involved in SolarWinds hack // ZDNet (https://www.zdnet.com/article/jetbrains-denies-being-involved-in-solarwinds-hack/). 07.01.2021).***

***

«По поручению президента Трампа сотрудники Совета национальной безопасности создали рабочую группу, известную как Cyber Unified Coordination Group (UCG), в состав которой входят ФБР, CISA и ODNI при поддержке NSA, для координации расследования и исправления ситуации, возникшей из-за значительного киберинцидента с участием сетей федерального правительства. UCG все еще работает над пониманием масштабов инцидента, но имеет следующие обновления о своих усилиях по расследованию и смягчению последствий.

Эта работа указывает на то, что субъект Advanced Persistent Threat (APT), вероятно, по происхождению российский, несет ответственность за большую часть или все недавно обнаруженные продолжающиеся кибер-компромиссы как в правительственных, так и в негосударственных сетях. В настоящее время мы полагаем, что это была и остается попытка сбора разведданных. Мы предпринимаем все необходимые шаги, чтобы понять весь масштаб этой кампании и отреагировать соответствующим образом.

UCG полагает, что из примерно 18 000 заказчиков продукта Orion компании Solar Winds в государственном и частном секторе, гораздо меньшее число пострадало в результате последующих действий в их системах. На данный момент мы определили менее десяти государственных агентств США, которые попадают в эту категорию, и работаем над выявлением и уведомлением неправительственных организаций, которые также могут быть затронуты.

Это серьезный компромисс, для исправления которого потребуются постоянные и целенаправленные усилия. С момента своего первоначального открытия UCG, включая трудолюбивых профессионалов из правительства Соединенных Штатов, а также наших партнеров из частного сектора, работали без перерыва. Эти усилия не утихли даже в праздничные дни. UCG будет продолжать принимать все необходимые меры для расследования, исправления и обмена информацией с нашими партнерами и американским народом.

Как ведущее агентство по реагированию на угрозы, расследование ФБР в настоящее время сосредоточено на четырех важнейших направлениях деятельности: выявление жертв, сбор доказательств, анализ доказательств для определения дальнейшей атрибуции и обмен результатами с нашими партнерами из правительства и частного сектора для информирования операций, разведывательная картина и сетевая защита.

Как лидер по реагированию на активы, CISA сосредоточена на быстром обмене информацией с нашими партнерами в правительстве и частном секторе, поскольку мы работаем над пониманием масштабов этой кампании и уровня эксплуатации. CISA также создала бесплатный инструмент для обнаружения необычной и потенциально вредоносной активности, связанной с этим инцидентом. В чрезвычайной директиве, опубликованной 14 декабря, CISA предписывает быстрое отключение или отключение питания затронутых продуктов SolarWinds Orion от федеральных сетей. CISA также выпустила техническое предупреждение, содержащее технические подробности и стратегии смягчения, чтобы помочь защитникам сети принять немедленные меры. CISA будет продолжать делиться известными подробностями по мере их появления.

ODNI, как руководитель службы разведки и связанной с ней деятельности, координирует работу разведывательного сообщества, чтобы гарантировать, что UCG располагает самой последней информацией, необходимой для принятия правительством США мер по смягчению последствий и реагированию. Кроме того, в рамках своей миссии по обмену информацией ODNI обеспечивает ситуационную осведомленность ключевых заинтересованных сторон и координирует деятельность по сбору разведывательных данных для устранения пробелов в знаниях.

Наконец, АНБ поддерживает UCG, предоставляя разведывательные данные, опыт в области кибербезопасности и практические рекомендации партнерам UCG, а также системам национальной безопасности, Министерству обороны и владельцам систем оборонной промышленной базы. Взаимодействие NSA как с UCG, так и с отраслевыми партнерами сосредоточено на оценке масштаба и размаха инцидента, а также на предоставлении технических мер по смягчению последствий.

UCG по-прежнему сосредоточена на обеспечении того, чтобы жертвы были идентифицированы и могли исправить свои системы, а доказательства были сохранены и собраны. Дополнительная информация, включая индикаторы компрометации, будет опубликована по мере ее появления». ***(JOINT STATEMENT BY THE FEDERAL BUREAU OF INVESTIGATION (FBI), THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA), THE OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), AND THE NATIONAL SECURITY AGENCY (NSA) // CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (https://www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure). 05.01.2021).***

***

«Четыре агентства кибербезопасности США, включая ФБР, CISA, ODNI и NSA, опубликовали сегодня совместное заявление, в котором официально обвиняют российское правительство в организации атаки на цепочку поставок SolarWinds.

Официальные лица США заявили, что «злоумышленник с повышенной устойчивой угрозой (APT), вероятно, русского происхождения» был ответственен за взлом SolarWinds, который чиновники описали как «попытку сбора разведданных».

Совместное заявление частично подтверждает отчет из Washington Post в прошлом месяце, который связан с SolarWinds вторжением в APT29, под кодовым именем, используемой в промышленности кибер-безопасности для описания хакеров, связанных с внешней разведки России (СВР).

Хотя официальные лица правительства США не связывают взлом SolarWinds с APT29 или какой-либо другой конкретной хакерской группой, это совместное заявление является ответом на публичную критику того, что администрация Трампа намеренно избегала приписывать атаку российским хакерам.

Эти слухи ходят в основном из-за предполагаемой связи и помощи, которую, как считается, президент Трамп получил от российских хакеров во время президентских выборов 2016 года.

Но совместное заявление касается и другого вопроса. В заявлении также формально описывается взлом SolarWinds как «усилие по сбору разведданных».

Официальные лица США надеются, что подобная категоризация взлома положит конец постоянным теориям заговора, распространяющимся в сети, о том, что целью взлома SolarWinds было вмешательство в работу машин для голосования и фальсификация выборов.

Кроме того, совместное заявление также пролило свет на ущерб от атаки.

Атака цепочки поставок SolarWinds произошла после того, как российские хакеры взломали внутреннюю инфраструктуру SolarWinds и добавили вредоносное ПО (названное Sunburst / Solorigate) в пакеты обновлений SolarWinds Orion.

Около 18 000 клиентов Orion получили и установили эти обновления, но только в некоторых из этих сетей российские хакеры решили усилить атаки с помощью вредоносного ПО второго уровня под названием Teardrop.

В то время как вредоносная нагрузка Sunburst первой стадии была обнаружена на тысячах систем, четыре агентства заявили, что «менее десяти правительственных агентств США» подверглись атакам дополнительных вредоносных программ.

Четыре агентства, стоящие за сегодняшним совместным заявлением, - это Агентство по кибербезопасности и безопасности инфраструктуры (CISA), Управление директора национальной разведки (ODNI) и Агентство национальной безопасности (NSA). Все четыре агентства являются членами Cyber Unified Coordination Group (UCG), совместной целевой группы, созданной Советом национальной безопасности Белого дома для расследования и устранения последствий атаки SolarWinds.

В сообщении в Facebook вскоре после публикации Washington Post в прошлом месяце российские официальные лица оспорили выводы газеты. Российские официальные лица официально не ответили на сегодняшнее совместное заявление ФБР-CISA-ODNI-NSA». ***(Catalin Cimpanu. US government formally blames Russia for SolarWinds hack // ZDNet (https://www.zdnet.com/article/us-government-formally-blames-russia-for-solarwinds-hack/). 05.01.2021).***

***

«В день выборов генерал Пол М. Накасоне, главный кибервоин страны, сообщил, что борьба с российским вмешательством в президентскую кампанию принесла большие успехи и раскрыла онлайн-оружие, инструменты и торговлю другой стороной.

«Мы расширили нашу деятельность и чувствуем себя очень хорошо там, где мы сейчас находимся», - сказал он журналистам.

Восемь недель спустя генерал Накасоне и другие американские чиновники, ответственные за кибербезопасность, теперь поглощены тем, что они упускали как минимум девять месяцев: взломом, который, как сейчас считается, затронул более 250 федеральных агентств и предприятий, и который Россия нацелил не на избирательную систему но в остальном правительство США и многие крупные американские корпорации.

Спустя три недели после того, как о вторжении стало известно, американские официальные лица все еще пытаются понять, было ли то, что осуществили русские, просто шпионской операцией внутри систем американской бюрократии или чем-то более зловещим, вставляя «черный ход» в правительственные учреждения, крупные корпорации., электросеть и лаборатории, разрабатывающие и транспортирующие ядерное оружие нового поколения.

Как минимум, это вызвало тревогу об уязвимости государственных и частных сетей в Соединенных Штатах для атак и подняло вопросы о том, как и почему национальная киберзащита провалилась так эффектно.

Эти вопросы приобрели особую актуальность, учитывая, что нарушение не было обнаружено ни одним из правительственных агентств, которые разделяют ответственность за киберзащиту - военным Киберкомандованием и Агентством национальной безопасности, оба из которых находятся в ведении генерала

Накасоне, и Министерством внутренних дел. Безопасность - но от частной компании по кибербезопасности FireEye.

«Это выглядит намного, намного хуже, чем я первоначально опасался», - сказал сенатор Марк Уорнер, демократ от Вирджинии и высокопоставленный член сенатского комитета по разведке. «Его размер продолжает увеличиваться. Ясно, что правительство Соединенных Штатов это упустило».

«И если бы FireEye не выступил», - добавил он, - «я не уверен, что мы до сих пор полностью осознаем это».

Интервью с ключевыми игроками, расследующими то, что спецслужбы считают операцией российской разведки СВР, выявили следующие моменты:

Нарушение намного шире, чем предполагалось. По первоначальным оценкам, Россия направила свои зонды только в несколько десятков из 18 000 государственных и частных сетей, к которым они получили доступ, когда вставили код в программное обеспечение для управления сетью, созданное техасской компанией SolarWinds. Но по мере того, как такие компании, как Amazon и Microsoft, которые предоставляют облачные сервисы, копают все глубже в поисках доказательств, теперь выясняется, что Россия использовала несколько уровней цепочки поставок, чтобы получить доступ к целым 250 сетям.

Хакеры управляли вторжением с серверов в Соединенных Штатах, используя юридические запреты Агентству национальной безопасности на участие во внутреннем слежении и уклонение от киберзащиты, развернутой Министерством внутренней безопасности.

Датчики «раннего предупреждения», размещенные киберкомандованием и Агентством национальной безопасности глубоко внутри иностранных сетей для обнаружения назревающих атак, явно не дали результата. Также пока нет никаких указаний на то, что какой-либо человеческий интеллект предупредил Соединенные Штаты о взломе.

Акцент правительства на защите на выборах, хотя и имеет решающее значение в 2020 году, возможно, отвлек ресурсы и внимание от давно назревающих проблем, таких как защита «цепочки поставок» программного обеспечения. В частном секторе компании, которые были сосредоточены на безопасности выборов, такие как FireEye и Microsoft, теперь раскрывают, что они были взломаны в рамках более крупной атаки на цепочку поставок.

SolarWinds, компания, которую хакеры использовали в качестве проводника для своих атак, в прошлом имела слабую безопасность своих продуктов, что делало ее легкой мишенью, по мнению нынешних и бывших сотрудников и государственных следователей. Ее исполнительный директор Кевин Б. Томпсон, который уходит с работы через 11 лет, уклонился от вопроса о том, должна ли его компания обнаруживать вторжение.

Часть скомпрометированного программного обеспечения SolarWinds была спроектирована в Восточной Европе, и в настоящее время американские следователи выясняют, возникло ли вторжение там, где глубоко укоренились оперативники российской разведки.

Намерения нападения остаются скрытыми. Но с приходом к власти новой администрации через три недели некоторые аналитики говорят, что русские,

возможно, пытаются поколебать уверенность Вашингтона в безопасности своих коммуникаций и продемонстрировать свой киберарсенал, чтобы получить рычаги воздействия на избранного президента Джозефа Р. Байдена-младшего перед переговорами по ядерному оружию.

«Мы до сих пор не знаем, каковы были стратегические цели России», - сказала Сюзанна Сполдинг, которая была старшим кибер-чиновником Министерства внутренней безопасности при администрации Обамы. «Но мы должны быть обеспокоены тем, что часть этого может выйти за рамки разведки. Их цель может заключаться в том, чтобы получить рычаги влияния на новую администрацию, например, приставить пистолет к нашей голове, чтобы удержать нас от действий, направленных против Путина».

Растущий список попаданий

Правительство США явно было в центре внимания атаки, при этом подтверждено, что в них проникли министерство финансов, госдепартамент, министерство торговли, министерство энергетики и части Пентагона. (Министерство обороны настаивает на том, что атаки на его системы не увенчались успехом, хотя и не представило никаких доказательств.)

Но взлом также затронул большое количество корпораций, многие из которых еще не сделали шаг вперед. SolarWinds считается одним из нескольких поставщиков цепочек поставок, которых Россия использовала для взлома. Microsoft, которая насчитала 40 жертв по состоянию на 17 декабря, сначала заявила, что взлома не было, но на этой неделе обнаружила, что это было - и что реселлеры ее программного обеспечения тоже. Ранее не сообщавшаяся оценка группы разведки Amazon показала, что число жертв могло быть в пять раз больше, хотя официальные лица предупреждают, что некоторые из них могут быть учтены дважды.

Официально официальные лица заявили, что не верят, что хакеры из СВР России взломали секретные системы, содержащие конфиденциальные сообщения и планы. Но в частном порядке официальные лица говорят, что у них до сих пор нет четкого представления о том, что могло быть украдено.

Они сказали, что их беспокоят деликатные, но несекретные данные, которые хакеры могли получить от таких жертв, как Федеральная комиссия по регулированию энергетики, включая Black Start, подробные технические чертежи того, как Соединенные Штаты планируют восстановить электричество в случае катастрофического отключения электроэнергии.

В планах России будет составлен список систем, на которые нужно нацелить, чтобы предотвратить восстановление электроэнергии в результате атаки, подобной той, которую она осуществила на Украине в 2015 году, отключив электричество на шесть часов в разгар зимы. Москва давно внедрила вредоносное ПО в американские электросети, а Соединенные Штаты сделали то же самое с Россией в качестве сдерживающего фактора.

Нарушение цепочки поставок

Основным объектом расследования до сих пор была компания SolarWinds, базирующаяся в Остине, чье программное обеспечение обновляет хакеры.

Но отдел кибербезопасности Министерства внутренней безопасности пришел к выводу, что хакеры работали и по другим каналам. А на прошлой неделе CrowdStrike, другая компания по безопасности, сообщила, что она также была безуспешно атакована теми же хакерами, но через компанию, которая занимается перепродажей программного обеспечения Microsoft.

Поскольку реселлерам часто поручают настраивать клиентское программное обеспечение, они, как и SolarWinds, имеют широкий доступ к сетям клиентов Microsoft. В результате они могут стать идеальным троянским конем для российских хакеров. Представители разведки выразили недовольство тем, что Microsoft не обнаружила атаку раньше; компания, которая в четверг заявила, что хакеры просмотрели ее исходный код, не раскрыла, какие из ее продуктов были затронуты и как долго хакеры находились в ее сети.

«Они были нацелены на самые слабые места в цепочке поставок и через наши самые надежные отношения», - сказал Гленн Чисхолм, основатель Obsidian Security.

Интервью с нынешними и бывшими сотрудниками SolarWinds показывают, что она не спешила делать безопасность приоритетом, хотя ее программное обеспечение было принято ведущей американской компанией по кибербезопасности и федеральными агентствами.

Сотрудники говорят, что под руководством г-на Томпсона, бухгалтера по образованию и бывшего финансового директора, каждая часть бизнеса была проверена на предмет экономии, а общие методы обеспечения безопасности были исключены из-за их расходов. Его подход помог почти утроить годовой доход SolarWinds до более чем 453 миллионов долларов в 2019 году со 152 миллионов долларов в 2010 году.

Но некоторые из этих мер могли подвергнуть компанию и ее клиентов большему риску нападения. SolarWinds переместила большую часть своего инжиниринга в вспомогательные офисы в Чешской Республике, Польше и Беларуси, где инженеры имели широкий доступ к программному обеспечению для управления сетью Orion, взломанному российскими агентами.

Компания только заявила, что манипулирование ее программным обеспечением было делом рук хакеров, а не компьютерной программы. Он не рассматривал публично возможность участия инсайдера в нарушении.

Ни один из клиентов SolarWinds, с которыми в последние недели связалась New York Times, не знал, что они полагаются на программное обеспечение, поддерживаемое в Восточной Европе. Многие говорили, что до недавнего времени даже не знали, что используют программное обеспечение SolarWinds.

По словам сотрудников, даже при том, что ее программное обеспечение установлено во всех федеральных сетях, SolarWinds взялась за безопасность только в 2017 году под угрозой наказания в соответствии с новым европейским законом о конфиденциальности. Только тогда, по словам сотрудников, SolarWinds наняла своего первого директора по информационным технологиям и назначила вице-президента по «архитектуре безопасности».

Ян Торнтон-Трамп, бывший советник по кибербезопасности в SolarWinds, сказал, что он предупреждал руководство в том году, что, если оно не проявит

более проактивный подход к своей внутренней безопасности, эпизод кибербезопасности будет «катастрофическим». После того как его основные рекомендации были проигнорированы, Торнтон-Трамп покинул компанию.

SolarWinds отказалась отвечать на вопросы об адекватности своей безопасности. В заявлении говорится, что он стал «жертвой изощренной, сложной и целенаправленной кибератаки» и тесно сотрудничал с правоохранительными органами, спецслужбами и экспертами по безопасности для расследования.

Но эксперты по безопасности отмечают, что после обнаружения российской атаки прошло несколько дней, прежде чем веб-сайты SolarWinds перестали предлагать клиентам скомпрометированный код.

Нападение важнее защиты

В последние годы миллиарды долларов из бюджета кибербезопасности были потрачены на программы наступательного шпионажа и упреждающих действий, что генерал Накасоне называет необходимостью «защищаться вперед», взламывая сети злоумышленников, чтобы заблаговременно изучить их операции и противодействовать им. внутри своих сетей, прежде чем они смогут атаковать, если потребуется.

Но этот подход, хотя и приветствовался как давно назревшая стратегия предотвращения атак, упустил возможность прорыва со стороны России.

По данным FireEye, устраивая свои атаки с серверов в Соединенных Штатах, в некоторых случаях используя компьютеры в том же городе или городе, что и их жертвы, русские воспользовались ограничением полномочий Агентства национальной безопасности. Конгресс не давал агентству или национальной безопасности никаких полномочий входить в сети частного сектора или защищать их. Именно в этих сетях оперативники CBP были менее осторожны, оставляя подсказки о своих вторжениях, которые FireEye в конечном итоге смог найти.

Вставив себя в обновление Orion SolarWinds и используя специальные инструменты, они также избежали срабатывания сигнализации системы обнаружения «Эйнштейн», которую национальная служба безопасности развернула в государственных учреждениях для обнаружения известных вредоносных программ, и так называемой программы CDM, которая была специально разработана для предупреждения агентств о подозрительной деятельности.

Некоторые сотрудники спецслужб задаются вопросом, было ли правительство настолько сосредоточено на вмешательстве в выборы, что открыло лазейки в других местах.

Спецслужбы несколько месяцев назад пришли к выводу, что Россия определила, что не может проникнуть в избирательные системы, достаточное для того, чтобы повлиять на результаты выборов, и вместо этого переключила свое внимание на отражение атак программ-вымогателей, которые могли лишить избирательных прав избирателей, и повлиять на операции, направленные на посеивание разногласий, разжигая сомнения в эффективности системы. честность и изменение мнения избирателей.

Взлом SolarWinds, начавшийся еще в октябре 2019 года, и вторжение в торговых посредников Microsoft дали России возможность атаковать наиболее уязвимые и наименее защищенные сети в нескольких федеральных агентствах.

Генерал Накасонэ отказался от интервью. Но представитель Агентства национальной безопасности Чарльз К. Штадтландер сказал: «Мы не рассматриваем это как компромисс «либо-либо». Действия, идеи и новые рамки, созданные в ходе усилий по обеспечению безопасности на выборах, имеют широкое положительное влияние на позицию страны и правительства США в области кибербезопасности».

Фактически, Соединенным Штатам, похоже, удалось убедить Россию в том, что атака, направленная на изменение голосов, вызовет дорогостоящий ответный удар. Но по мере того, как становится очевидным масштаб вторжения, становится ясно, что американскому правительству не удалось убедить Россию, что широкомасштабный взлом федерального правительства и корпоративных сетей приведет к аналогичным последствиям.

Избавление от хакеров

Представители разведки говорят, что могут пройти месяцы, а то и годы, прежде чем они получат полное представление о взломе.

После того, как в 2017 году был задержан один из ведущих осведомителей Кремля, осведомленность ЦРУ о российских операциях уменьшилась. По словам представителей разведки, СВР остается одной из самых эффективных разведывательных служб в мире, избегая электронных коммуникаций, которые могут раскрыть ее секреты Агентству национальной безопасности.

Наилучшие оценки СВР дали голландцы. В 2014 году хакеры, работающие на Голландскую службу общей разведки и безопасности, взломали компьютеры, используемые группой, наблюдая за ними не менее года, а в какой-то момент ловили их на камеру.

Именно голландцы помогли предупредить Белый дом и Государственный департамент о взломе их систем СВР в 2014 и 2015 годах, а в прошлом месяце они поймали и выслали из Нидерландов двух сотрудников СВР, обвиненных в проникновении туда технологических компаний. Хотя известно, что эта группа не является деструктивной, ее крайне сложно изгнать из компьютерных систем, в которые она проникла.

Когда СВР взломала несекретные системы Госдепартамента и Белого дома, Ричард Леджетт, тогдашний заместитель директора Агентства национальной безопасности, сказал, что агентство занялось цифровым эквивалентом «рукопашного боя». В какой-то момент СВР получила доступ к инструменту NetWitness Investigator, который следователи используют для выкорчевывания черных дверей в России, манипулируя им таким образом, чтобы хакеры продолжали уклоняться от обнаружения.

Следователи заявили, что они предположили, что они выгнали СВР, но обнаружили, что группа проникла через другую дверь.

Некоторые эксперты по безопасности сказали, что избавление стольких разрозненных федеральных агентств от СВР может быть бесполезным и что единственный путь вперед может заключаться в том, чтобы отключить системы и начать заново. Другие заявили, что делать это в разгар пандемии будет непомерно дорого и отнимет много времени, и новой администрации придется поработать над выявлением и сдерживанием каждой скомпрометированной системы, прежде чем она сможет откалибровать ответ.

«SVR является преднамеренным, изощренным, и у них нет таких юридических ограничений, как у нас здесь, на Западе», - сказал Адам Дарра, бывший аналитик правительственной разведки, который сейчас является директором разведки в Vigilante, охранной фирме.

Он добавил, что санкции, обвинительные заключения и другие меры не смогли остановить СВР, которая показала, что она может быстро адаптироваться.

«Они сейчас очень внимательно следят за нами», - сказал г-н Дарра. «И они будут меняться соответственно». ***(David E. Sanger, Nicole Perlroth, Julian E. Barnes. As Understanding of Russian Hacking Grows, So Does Alarm // The New York Times Company (https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html). 02.01.2021).***

***

«Одна из самых неприятных вещей в атаке SolarWinds заключалась в том, что русская трещина оставалась незамеченной с марта по декабрь 2020 года. В то время взлом SolarWinds, совершенный российским правительством, открывал дверь к секретам многочисленных ведущих американских правительственных агентств и технологических компаний. Даже сейчас мы все еще пытаемся понять, насколько широко и ужасно были трещины SolarWinds.

Основными причинами этой трещины были опасные сбои в цепочке поставок программного обеспечения. Для SolarWinds уже слишком поздно что-либо делать, кроме контроля повреждений, но Linux Foundation нашла несколько уроков, чтобы убедиться, что ваши программы, будь то с открытым исходным кодом или проприетарные, избегают катастроф в стиле SolarWinds.

Дэвид А. Уилер, директор Linux Foundation по безопасности цепочки поставок с открытым исходным кодом, объяснил, что во время атаки Orion вредоносный код был вставлен в Orion путем подрыва среды сборки программы. Это процесс, в котором программа компилируется из исходного кода в двоичную исполняемую программу, развертываемую конечными пользователями. В этом случае компания по безопасности CrowdStrike выяснила, что вредоносная программа Sunspot наблюдала за сервером сборки на предмет команд сборки и незаметно заменяла некоторые файлы исходного кода Orion вредоносными программами.

Входя в программу еще до того, как она станет полноценной программой, этот взлом делает большинство обычных рекомендаций по безопасности бесполезными. Например,

«Устанавливать только подписанные версии» не помогает, потому что это программное обеспечение было подписано.

«Обновите программное обеспечение до последней версии» не помогает, потому что обновленное программное обеспечение было подделано.

«Мониторинг поведения программного обеспечения» в конце концов обнаружил проблему, но атака была довольно скрытной и была обнаружена только после того, как был нанесен огромный ущерб.

«Обзор исходного кода» тоже не является верной защитой. В случае с Орионом даже нельзя быть уверенным, что разработчики могли заметить

изменения исходного кода. Изменения были тщательно написаны, чтобы выглядеть как ожидаемый код. Кроме того, поскольку злоумышленники контролировали среду сборки, они могли внедрить атаку, не будучи видимыми разработчикам программного обеспечения.

Наконец, поскольку Orion не является программным обеспечением с открытым исходным кодом, никто не может проводить независимую проверку кода. Только разработчики компании могли просматривать его или его систему сборки и конфигурации. Как сказал Уиллер: «Если нам потребовались дополнительные доказательства того, что неясность исходного кода программного обеспечения не обеспечивает автоматически безопасность, то вот оно».

Так что ты можешь сделать? Что ж, использование открытого исходного кода - хорошее начало. В методологии открытого исходного кода нет ничего волшебного. Ошибки безопасности все еще могут ввести код, но, по крайней мере, у вас есть возможность искать проблемы, прежде чем они взорвутся.

Кроме того, как указал Уиллер, компании должны укрепить свою среду сборки от злоумышленников. Например, SolarWinds использовала крайне плохие методы обеспечения безопасности разработчиков. Это включало использование небезопасного протокола ftp для передачи файлов и публичное раскрытие паролей. Любая среда сборки, все еще использующая их, просто требует нарушения безопасности.

Системы сборки являются критически важными производственными системами, и к ним следует относиться так же. Во всяком случае, они должны получать более высокий уровень требований безопасности, чем производственные среды. Это безопасность кода 101.

Даже когда вы максимально обезопасили свою систему сборки, не факт, что она безопасна. В конечном счете, Уиллер считает, что есть только одна по-настоящему сильная контрмера для такого рода атак: проверенные воспроизводимые сборки.

«Воспроизводимая сборка, - писал Уиллер, - это та, которая» всегда дает одни и те же выходные данные при одинаковых входных данных, так что результаты сборки могут быть проверены. Проверенная воспроизводимая сборка - это процесс, при котором независимые организации создают сборку из исходного кода и проверяют, что полученные результаты взяты из заявленного исходного кода».

Это более хорошая идея, чем то, что вы можете сделать сегодня. Сегодня очень мало программ можно проверить. Linux Foundation и Civil Infrastructure Platform финансируют работу, в том числе проект воспроизводимых сборок, по созданию проверенных воспроизводимых сборок.

Linux Foundation хочет, чтобы все начали внедрять и требовать проверенных воспроизводимых сборок. Да, это будет непросто. Большая часть программного обеспечения не предназначена для воспроизведения в среде сборки. На создание воспроизводимого программного обеспечения могут уйти годы.

Уиллер писал:

Чтобы сделать программное обеспечение воспроизводимым, необходимо внести много изменений, поэтому часто требуются ресурсы (время и деньги). И

есть много программного обеспечения, которое необходимо воспроизводить, включая пакеты операционной системы и пакеты уровня библиотеки. Существуют системы распространения пакетов, которые необходимо будет пересмотреть и, вероятно, изменить. Я ожидал бы, что некоторые из наиболее важных программ сначала станут воспроизводимыми, а затем со временем будут увеличиваться менее важные программы по мере увеличения давления, чтобы сделать более воспроизводимое программное обеспечение, прошедшее проверку. Было бы разумно разработать широко применимые стандарты и лучшие практики для создания воспроизводимых сборок. После того как программное обеспечение станет воспроизводимым, другим пользователям потребуется проверить результаты сборки для данного исходного кода, чтобы противостоять этим видам атак.

Воспроизводимые сборки намного проще для программного обеспечения с открытым исходным кодом (OSS), потому что нет никаких юридических препятствий для наличия большого количества верификаторов. Разработчики программного обеспечения с закрытым исходным кодом столкнутся с дополнительными проблемами; их бизнес-модели часто зависят от сокрытия исходного кода. По-прежнему возможно иметь «доверенных перекомпоновщиков» по всему миру для проверки программного обеспечения с закрытым исходным кодом, даже если это сложнее и количество перестроителей обязательно будет меньше.

Индустрия информационных технологий, как правило, отходит от «черных ящиков», которые нельзя проверить и проверить, к компонентам, которые можно проверять. Так что это часть общей тенденции отрасли; это тенденция, которую необходимо ускорить.

Не может быть? Почему бы и нет? Аудиторы имеют доступ к финансовым данным и проверяют финансовые системы большинства предприятий. Программным компаниям нужны аудиторы по программированию и построению. В противном случае мы наверняка увидим больше атак, направленных на создание программного обеспечения, которые распространяют вредоносное ПО.

Слишком дорогой? Подумай еще раз. SolarWinds уже попадает под действие своего первого коллективного иска. Больше будет позже. Акции компании также упали на 40% после того, как стало известно о ее банкротстве.

Уиллер также напомнил нам, что «злоумышленники всегда пойдут самым легким путем, поэтому мы не можем игнорировать другие атаки».

В частности, поскольку большинство атак используют непреднамеренные уязвимости в коде, мы должны предотвращать эти непреднамеренные уязвимости. Эти меры включают изменение инструментов и интерфейсов, чтобы избежать проблем; обнаружение остаточных уязвимостей перед развертыванием; и обучение разработчиков разработке безопасного программного обеспечения. Например, есть бесплатные курсы edX от Open Source Security Foundation (OpenSSF) о том, как разрабатывать безопасное программное обеспечение.

Уилер также отметил, что, поскольку «приложения в основном представляют собой повторно используемое программное обеспечение (с небольшим количеством настраиваемого кода), поэтому цепочка поставок этого повторно

используемого программного обеспечения имеет решающее значение. Повторно используемые компоненты часто чрезвычайно устарели. непреднамеренные уязвимости. В самом деле, повторно используемые компоненты с известными уязвимостями являются одними из самых верхних распространенных проблем в веб - приложениях. В инструменты Л.Ф. безопасности LFX, Dependabot GitHub в, анализаторы зависимостей GitLab в, и многие другие инструменты и услуги могут помочь обнаружить повторно использовать компоненты с известными уязвимостями».

Опять же, простое использование OSS не означает, что это безопасно. Уиллер добавил: «Уязвимости в широко повторно используемых OSS могут вызывать широко распространенные проблемы, поэтому LF работает над выявлением таких OSS, чтобы их можно было проанализировать и укрепить».

Даже если вы используете проприетарные программы, исходный код может быть открытым. Synopsys обнаружила, что 99% коммерческих программ включают как минимум один компонент с открытым исходным кодом. Это нормально, но 91% из них содержат устаревший или заброшенный код с открытым исходным кодом. Это совсем не хорошо.

Вредоносный код также может скрываться в цепочке поставок. Например, как заявил Уилер, «большая часть вредоносного кода попадает в приложения через "typosquatting" библиотеки. То есть путем создания вредоносной библиотеки с именем, которое выглядит как легитимная библиотека».

Для пользователей это означает, что они должны начать запрашивать спецификацию программного обеспечения (SBOM), чтобы они точно знали, что они используют. Да, это еще один аргумент в пользу открытого кода. Орион, как и все проприетарное ПО, представляет собой черный ящик. Никто, кроме его строителей, не знает, что в нем. И с Орионом, похоже, они никогда не знали ни того, ни другого, пока он не взорвался в лицах их пользователей.

Национальная администрация по телекоммуникации и связи и информации США (NTIA) обнадеживает принятие SBOM. Формат обмена данными пакетов программного обеспечения (SPDX) Linux Foundation - это широко распространенный формат SBOM.

Вооружившись информацией SBOM, вы можете проверить, какие версии компонентов используются в вашей программе. Конечно, это требует, чтобы вы обращали внимание на то, что находится в ваших программах. Например, печально известный провал Equifax был вызван тем, что он просто не обратил внимания, когда было выпущено публичное исправление для библиотеки Apache Struts, которую он использовал в своих программах. Equifax попытался свалить вину на Apache, но когда пыль улеглась, Equifax признал, что полностью виноват.

Когда в программе используются компоненты с известными уязвимостями, это большой красный флаг. Правда, некоторые уязвимости могут быть недоступны для использования, но, как утверждает Уилер, «слишком многие разработчики приложений просто не обновляют зависимости, даже если они могут быть использованы., здесь есть проблема курицы и яйца: спецификации находятся в процессе обновления, инструменты находятся в разработке, и многие производители программного обеспечения не готовы предоставить SBOM.

Поэтому пользователям не следует ожидать, что большинство производителей программного обеспечения будут иметь готовые SBOM. сегодня. Тем не менее, им необходимо создать спрос на SBOM».

Уилер также хочет, чтобы дистрибьюторы программного обеспечения использовали информацию о SBOM. «Для многих проектов OSS это обычно можно сделать, по крайней мере частично, путем предоставления информации об управлении пакетами, которая определяет их прямые и косвенные зависимости (например, в package.json, requirements.txt, Gemfile, Gemfile.lock и подобных файлах) Многие инструменты могут комбинировать эту информацию для создания более полной информации SBOM для более крупных систем».

Наконец, Уиллер считает: «Организации должны инвестировать в соответствие OpenChain и требовать от своих поставщиков внедрения процесса, направленного на повышение доверия к цепочке поставок». OpenChain - это технология распределенного реестра с открытым исходным кодом, защищенная блокчейном, для отслеживания программных компонентов и лицензий с открытым исходным кодом. Это также стандарт ISO / IEC: 5230: 2020.

Имея это в виду, вам следует включить все перечисленное ниже в свой список разработки и развертывания программного обеспечения:

Усиление среды сборки программного обеспечения

Переходите к проверенным воспроизводимым сборкам

Измените инструменты и интерфейсы, чтобы снизить вероятность непреднамеренных уязвимостей

Обучайте разработчиков

Используйте инструменты обнаружения уязвимостей при разработке программного обеспечения

Используйте инструменты для обнаружения известных уязвимых компонентов при разработке программного обеспечения

Улучшение широко используемых OSS

Спрашивайте SBOM в формате SPDX. Многие производители программного обеспечения еще не готовы предоставить его, но создание спроса ускорит прогресс.

Определите, есть ли в используемых субкомпонентах известные уязвимости

Работать над предоставлением информации SBOM, если мы производим программное обеспечение для других

Внедрить OpenChain

Если вы этого не сделаете, как напоминает нам Уиллер, «те, кто не извлекает уроки из истории, часто обречены повторять ее». Вы хотите, чтобы ваша компания стала следующей компанией SolarWinds? Я так не думаю!» ***(Steven J. Vaughan-Nichols. SolarWinds defense: How to stop similar attacks // ZDNet (https://www.zdnet.com/article/solarwinds-defense-how-to-stop-similar-attacks/). 14.01.2021).***

***

«Фирма по кибербезопасности CrowdStrike, одна из компаний, непосредственно участвующих в расследовании атаки на цепочку поставок

SolarWinds, заявила сегодня, что обнаружила третий штамм вредоносного ПО, непосредственно участвовавший в недавнем взломе.

Названная Веснушка, эта находка добавляет к ранее обнаруженному Sunburst (Solorigate) и штаммам Teardrop вредоносных программ.

Но в то время как Sunspot является последним открытием взлома SolarWinds, Crowdstrike заявила, что на самом деле вредоносная программа была использована первой.

ВРЕДОНОСНОЕ ПО SUNSPOT ЗАПУСКАЛОСЬ НА СЕРВЕРЕ СБОРКИ SOLARWINDS

В опубликованном сегодня отчете Crowdstrike говорится, что Sunspot был развернут в сентябре 2019 года, когда хакеры впервые взломали внутреннюю сеть SolarWinds.

Вредоносная программа Sunspot была установлена на сервере сборки SolarWinds, типе программного обеспечения, используемом разработчиками для сборки более мелких компонентов в более крупные программные приложения.

CrowdStrike сказал, что Sunspot преследовал одну единственную цель, а именно - следить за сервером сборки для команд сборки, которые собирают Orion, один из лучших продуктов SolarWinds, платформу мониторинга ИТ-ресурсов, используемую более чем 33 000 клиентов по всему миру.

После обнаружения команды сборки вредоносная программа незаметно заменяла файлы исходного кода внутри приложения Orion файлами, загружающими вредоносное ПО Sunburst, в результате чего создавались версии приложения Orion, которые также устанавливали вредоносное ПО Sunburst.

ХРОНОЛОГИЯ АТАКИ НА ЦЕПОЧКУ ПОСТАВОК SOLARWINDS

Эти троянизированные клиенты Orion в конечном итоге попали на один из официальных серверов обновлений SolarWinds и были установлены в сетях многих клиентов компании.

Как только это произойдет, вредоносная программа Sunburst активируется во внутренних сетях компаний и государственных учреждений, где она будет собирать данные о своих жертвах, а затем отправлять информацию обратно хакерам SolarWinds (см. Этот отчет Symantec о том, как данные были отправлены обратно через DNS-запрос.).

Затем злоумышленники решали, была ли жертва достаточно важной для компрометации, и развертывали в этих системах более мощный бэкдорный троян Teardrop, одновременно давая команду Sunburst удалить себя из сетей, которые он считал незначительными или слишком опасными.

Однако сообщение о том, что в результате атаки SolarWinds была обнаружена третья вредоносная программа, является одним из трех основных обновлений, появившихся сегодня в связи с этим инцидентом.

В отдельном объявлении, опубликованном в своем блоге, SolarWinds также опубликовала хронологию взлома. Поставщик программного обеспечения из Техаса заявил, что до того, как вредоносное ПО Sunburst было развернуто для клиентов в период с марта по июнь 2020 года, хакеры также провели тестовый запуск в период с сентября по ноябрь 2019 года.

«Следующая версия релиза платформы Orion от октября 2019 года, по-видимому, содержала модификации, предназначенные для проверки способности злоумышленников вставлять код в наши сборки», - заявил сегодня генеральный директор SolarWinds Судхакар Рамакришна в оценке, также отраженной в отчете CrowdStrike.

КОД ПЕРЕКРЫВАЕТСЯ С ВРЕДОНОСНЫМ ПО TURLA

Кроме того, компания по безопасности Kaspersky также опубликовала свои собственные выводы ранее в этот же день в отдельном отчете.

Kaspersky, который не участвовал в формальном расследовании атаки SolarWinds, но все же проанализировал вредоносное ПО, заявил, что он изучил исходный код вредоносного ПО Sunburst и обнаружил перекрытие кода между Sunburst и Kazuar, разновидностью вредоносных программ, связанных с группой Turla, Россия. самая изощренная кибершпионажная организация, спонсируемая государством.

Сегодня Касперский был очень осторожен в своем языке, чтобы указать, что он обнаружил только «перекрытия кода», но не обязательно полагает, что группа Turla организовала атаку SolarWinds.

Фирма по безопасности утверждала, что это перекрытие кода могло быть результатом того, что хакеры SolarWinds использовали одни и те же идеи кодирования, покупали вредоносное ПО у одного и того же кодировщика, кодировщики перемещались между разными участниками угроз, или могло быть просто операцией ложного флага, призванной привести охранные фирмы к неверный путь.

Но хотя охранные фирмы воздерживаются от обвинений, на прошлой неделе официальные лица правительства США официально обвинили Россию во взломе SolarWinds, назвав хакеров «вероятно, русскими по происхождению».

В заявлении правительства США взломанная группа не указана. Некоторые новостные агентства связывают атаку с группой, известной как APT29 (или Cozy Bear), но все охранные фирмы и исследователи безопасности, участвовавшие в взломе, призвали к осторожности и очень робко относились к такому раннему официальному отнесению взлома к определенной группе в расследовании.

Сейчас хакеры SolarWinds отслеживаются под разными именами, такими как UNC2452 (FireEye, Microsoft), DarkHalo (Volexity) и StellarParticle (CrowdStrike), но ожидается, что это обозначение изменится, когда компании узнают больше.

Прямо сейчас остается одна последняя загадка: как хакерам SolarWinds удалось взломать сеть компании и установить вредоносное ПО Sunspot. Была ли это незащищенная VPN, целенаправленная фишинговая атака по электронной почте или сервер, который оставался открытым с угадываемым паролем?» ***(Catalin Cimpanu. Third malware strain discovered in SolarWinds supply chain attack // ZDNet (https://www.zdnet.com/article/third-malware-strain-discovered-in-solarwinds-supply-chain-attack/). 12.01.2021).***

***

«Веб-сайт под названием SolarLeaks продает данные, которые, как они утверждают, были украдены у компаний, которые, как подтверждено, были взломаны в результате атаки SolarWinds.

В прошлом месяце стало известно, что компания по управлению сетью SolarWinds подверглась сложной кибератаке, которая привела к атаке на цепочку поставок, затронувшей 18 000 клиентов.

Согласно совместному заявлению ФБР, CISA и АНБ, эта атака «вероятно» была проведена спонсируемой российским государством хакерской группой, которая хотела украсть облачные данные, такие как электронная почта и файлы, у своих жертв.

Сегодня был запущен веб-сайт solarleaks [.] Net, который утверждает, что продает украденные данные от Microsoft, Cisco, FireEye и SolarWinds. Известно, что все эти компании были взломаны во время атаки на цепочку поставок.

Сайт утверждает, что продает исходный код и репозитории Microsoft за 600 000 долларов. Microsoft подтвердила, что злоумышленники получили доступ к их исходному коду во время взлома SolarWinds…

Злоумышленники также заявляют, что продают исходный код для нескольких продуктов Cisco, что еще больше касается внутреннего средства отслеживания ошибок компании…

В обновленном сегодня информационном сообщении Cisco заявляет, что им известно о сайте SolarLeaks и что нет никаких доказательств того, что злоумышленники украли их исходный код.

"Cisco осведомлена об этом веб-сайте и на данный момент не имеет доказательств какой-либо кражи интеллектуальной собственности, связанной с недавними событиями. Мы стремимся к прозрачности, и если мы найдем информацию, которую должны знать наши клиенты, мы поделимся ею через наш установленный каналов ", - говорится в сообщении Cisco.

Веб-сайт также утверждает, что продает частные инструменты красной команды, а исходный код, который, как сообщила FireEye, был украден во время их атаки, за 50 000 долларов…

Наконец, на сайте продается исходный код SolarWinds и дамп клиентского портала за 250 000 долларов…

На сайте говорится, что за 1 миллион долларов вы получите все утекшие данные.

В стиле, аналогичном Shadow Brokers, участники SolarLeaks заявляют, что они будут продавать украденные данные партиями, и позже будет выпущено больше.

Домен solarleaks.net зарегистрирован через NJALLA, известного регистратора, используемого российскими хакерскими группами Fancy Bear и Cozy Bear.

При просмотре записи WHOIS для сети solarleaks [.], Назначенные серверы имен также дразнят исследователей заявлением «Вы не можете получить информацию».

Не подтверждено, является ли этот сайт законным и есть ли у владельцев сайтов данные, которые они продают.

Президент Rendition Infosec Джейк Уильямс заявляет, что сделка с упором на коммерчески ценные данные, а не на разведданные, украденные у государственных органов, может указывать на то, что это настоящая группа.

Когда мы попытались связаться с ними с вопросами, указанный адрес электронной почты был возвращен с ошибкой, что адрес электронной почты не существует…

Обновление 14.01.20: Со времени нашей первой статьи появилась дополнительная информация о сайте SolarLeaks…

13 января репортер Motherboard Vice Лоренцо Франчески-Биккьераи получил электронное письмо, в котором утверждалось, что он был от актеров SolarLeaks. На просьбу предоставить образец якобы украденных данных злоумышленники отказались предоставить какие-либо доказательства, поскольку это не «так просто».

Позже в тот же день сайт SolarLeaks был обновлен, чтобы включить новое сообщение о том, что ProtonMail отключил свою электронную почту и что покупатели, которые хотят увидеть образец данных, должны отправить 100 XMR, или примерно 16000 долларов, на указанный адрес Monero…

Шестнадцатеричная «подсказка» внизу обновления выглядит как хеш SHA-256, но в настоящее время она не связана с известным файлом.

ProtonMail также подтвердил, что они заблокировали свою учетную запись в твите MalwareHunterTeam.

Хотя многие по-прежнему считают этот сайт мошенничеством, Microsoft странным образом начала обнаруживать зашифрованный архив, предположительно содержащий их исходный код как HackTool: Win32 / Solardump.A и HackTool: Win32 / Solardump.B.

Что еще хуже, сайт-подражатель в SolarLeak [.] Net был создан с тем же содержанием веб-сайта, но с другим адресом Monero». ***(Lawrence Abrams. SolarLeaks site claims to sell data stolen in SolarWinds attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/solarleaks-site-claims-to-sell-data-stolen-in-solarwinds-attacks/). 12.01.2021).***

***

«Как и предсказывалось большинством экспертов в прошлом месяце, последствия атаки на цепочку поставок SolarWinds со временем становятся все сильнее, и у компаний было время для аудита внутренних сетей и журналов DNS.

На этой неделе четыре новых поставщика кибербезопасности - Mimecast, Palo Alto Networks, Qualys и Fidelis - добавили свои имена в список компаний, которые установили троянизированные версии приложения SolarWinds Orion.

ВЗЛОМ MIMECAST СВЯЗАН С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ SOLARWINDS

Наиболее важные объявления на этой неделе были сделаны Mimecast, поставщиком продуктов для защиты электронной почты.

Две недели назад компания раскрыла серьезное нарушение безопасности, во время которого хакеры проникли в ее сеть и использовали цифровые сертификаты,

используемые одним из ее продуктов безопасности, для доступа к учетным записям Microsoft 365 некоторых из ее клиентов.

В сегодняшнем обновлении своего блога Mimecast сообщила, что связывает этот инцидент с троянизированным приложением SolarWinds Orion, установленным в его сети.

Теперь компания подтвердила, что хакеры SolarWinds - это те, кто злоупотребил ее сертификатом, чтобы преследовать клиентов Mimecast.

PALO ALTO NETWORKS РАСКРЫВАЕТ ИНЦИДЕНТЫ В СЕНТЯБРЕ И ОКТЯБРЕ 2020 ГОДА

Еще одним крупным поставщиком средств безопасности, который выступил с заявлением об инциденте, связанном с SolarWinds, был Palo Alto Networks, поставщик программного обеспечения для кибербезопасности и сетевого оборудования.

В беседе с журналистом-расследователем Forbes Томасом Брюстером на этой неделе Palo Alto Networks заявила, что в сентябре и октябре 2020 года обнаружила два инцидента безопасности, связанные с программным обеспечением SolarWinds.

«Наш Центр управления безопасностью [...] немедленно изолировал сервер, инициировал расследование и подтвердил, что наша инфраструктура безопасна», - сообщил Forbes в понедельник Palo Alto Networks.

Тем не менее, компания заявила, что расследовала нарушения как отдельные отдельные инциденты и не обнаружила более широкую атаку цепочки поставок, которая будет обнаружена только через несколько месяцев, когда хакеры взломали другого поставщика средств безопасности FireEye.

Palo Alto Networks заявила, что расследование вторжений, связанных с SolarWinds в сентябре и октябре, не принесло больших результатов и пришло к выводу, что «попытка атаки была неудачной и никакие данные не были скомпрометированы».

QUALYS: ЭТО БЫЛА ВСЕГО ЛИШЬ ТЕСТОВАЯ СИСТЕМА

Но в отчете Forbes также цитируются выводы Эрика Хьельмвика, основателя компании по сетевой безопасности Netresec, который опубликовал в понедельник отчет с подробным описанием 23 новых доменов, которые использовались хакерами SolarWinds для развертывания полезных нагрузок второго уровня в зараженных сетях, которые они считали очень ценными.

Два из этих 23 новых доменов были «corp.qualys.com», что свидетельствует о том, что злоумышленники могли стать объектом аудита кибербезопасности Qualys.

Однако в заявлении Forbes Qualys заявила, что вторжение было не таким масштабным, как кажется, и заявили, что его инженеры установили троянскую версию приложения SolarWinds Orion в лабораторной среде для целей тестирования, отдельно от основной сети.

По словам Qualys, последующее расследование не обнаружило никаких доказательств дальнейшей злонамеренной деятельности или кражи данных.

Однако некоторые исследователи безопасности не соглашаются с заявлением компании, предполагающим, что домен "corp.qualys.com" предполагает, что хакеры действительно получили доступ к его основной сети, а не к лабораторной среде, как заявляет компания.

FIDELIS ТАКЖЕ РАСКРЫВАЕТ ТАРГЕТИНГ НА ВТОРОМ ЭТАПЕ

Четвертая и последняя крупная информация была раскрыта сегодня от Fidelis Cybersecurity в форме сообщения в блоге от директора по информационной безопасности компании Криса Кубича.

Представитель Fidelis сказал, что они также установили троянизированную версию приложения SolarWinds Orion в мае 2020 года в рамках «оценки программного обеспечения».

«Установка программного обеспечения была отслежена до машины, настроенной как тестовая система, изолированной от нашей базовой сети и редко включаемой», - сказал Кубич.

Фиделис сказал, что, несмотря на попытки злоумышленника расширить свой доступ во внутреннюю сеть Fidelis, компания считает, что тестовая система была «достаточно изолирована и слишком редко включалась, чтобы злоумышленник мог перейти к следующему этапу атаки».

Раскрытие информации на этой неделе доводит общее количество поставщиков средств кибербезопасности, на которые нападут хакеры SolarWinds, до восьми. Предыдущие разоблачения исходили от FireEye (первоначальное вторжение, которое раскрыло всю атаку цепочки поставок SolarWinds), Microsoft (злоумышленники получили доступ к некоторому исходному коду компании), CrowdStrike (неудачное вторжение) и Malwarebytes (злоумышленники получили доступ к некоторым адресам электронной почты компании Счета)». ***(Catalin Cimpanu. Four security vendors disclose SolarWinds-related incidents // ZDNet (https://www.zdnet.com/article/four-security-vendors-disclose-solarwinds-related-incidents/). 26.01.2021).***

***

Кіберзахист критичної інфраструктури

«Морская отрасль - соблазнительная цель для хакеров. Один только порт Лос-Анджелеса (Порт) в прошлом году способствовал развитию торговли на сумму около 276 миллиардов долларов, а по оценкам Международной палаты судоходства, общая стоимость мирового судоходства в 2019 году составила около 14 триллионов долларов. Порт планирует построить многомиллионный порт. - долларовая киберразведка в качестве центра обмена информацией между государственным и частным секторами для предотвращения растущих атак на морскую отрасль и логистику. Этот центр, Центр киберустойчивости, является одним из первых в своем роде, построенных в США. Исполнительный директор порта Джин Серока сказал: «Со временем мы заметили, что потенциальные проникновения и киберугрозы растут каждый год», включая такие инциденты, как атаки NotPetya 2017 года, затронувшие судоходные линии, В 2018 году программа-вымогатель нацелена на порт Лонг-Бич, а в октябре 2020 года программа-вымогатель была атакована на французскую транспортную и контейнерную компанию CMA CGM SA. Серока сказал, что по мере того, как угроза становится все более очевидной, порту «необходимо найти способ привлечь частный сектор в

это пространство». Ожидается, что Центр киберустойчивости заработает к концу 2021 года. Участники этого обмена информацией смогут анонимно обмениваться информацией через платформу, которая стандартизирует данные из инструментов кибербезопасности различных компаний. Директор по информационным технологиям порта возглавит проект, который будет работать вместе с операционным центром кибербезопасности порта. французская транспортная и контейнерная компания. Серока сказал, что по мере того, как угроза становится все более очевидной, порту «необходимо найти способ привлечь частный сектор в это пространство». Ожидается, что Центр киберустойчивости заработает к концу 2021 года. Участники этого обмена информацией смогут анонимно обмениваться информацией через платформу, которая будет стандартизировать данные из инструментов кибербезопасности различных компаний. Директор по информационным технологиям порта возглавит проект, который будет работать вместе с операционным центром кибербезопасности порта. французская транспортная и контейнерная компания. Серока сказал, что по мере того, как угроза становится все более очевидной, порту «необходимо найти способ привлечь частный сектор в это пространство». Ожидается, что Центр киберустойчивости заработает к концу 2021 года. Участники этого обмена информацией смогут анонимно обмениваться информацией через платформу, которая будет стандартизировать данные из инструментов кибербезопасности различных компаний. Директор по информационным технологиям порта возглавит проект, который будет работать вместе с операционным центром кибербезопасности порта. Участники этого обмена информацией смогут анонимно обмениваться информацией через платформу, которая стандартизирует данные из инструментов кибербезопасности различных компаний. Директор по информационным технологиям порта возглавит проект, который будет работать вместе с операционным центром кибербезопасности порта. Участники этого обмена информацией смогут анонимно обмениваться информацией через платформу, которая стандартизирует данные из инструментов кибербезопасности различных компаний. Директор по информационным технологиям порта возглавит проект, который будет работать вместе с операционным центром кибербезопасности порта.

Серока сказал, что он надеется, что Центр киберустойчивости станет образцом для других крупных портов в Соединенных Штатах, поскольку обмен информацией является таким жизненно важным средством защиты. По мере того, как судоходная отрасль становится все более оцифрованной, киберугрозы потребуют таких средств, как порты, для определения приоритетов установленных стандартов данных, бизнес-правил и открытой архитектуры для обеспечения безопасного и защищенного обмена информацией». ***(KATHRYN RATTIGAN. Cyber Intelligence Facility in Port of Los Angeles to Thwart Maritime Threats // Robinson+Cole LLP. (https://www.dataprivacyandsecurityinsider.com/2021/01/cyber-intelligence-facility-in-port-of-los-angeles-to-thwart-maritime-threats/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+DataPrivacyAndSecurityInsider+%28Data+Privacy+%2B+Security+Insider%29). 07.01.2021).***

***

«Около миллиона скомпрометированных учетных записей, обеспечивающих внутренний доступ к компаниям, занимающимся видеоиграми, выставлены на продажу на форумах в даркнете, поскольку киберпреступники все чаще обращаются к индустрии онлайн-игр как к важной цели, заявила компания по безопасности.

К 2022 году выручка индустрии онлайн-игр должна составить почти 200 миллиардов долларов. Но, несмотря на это, в некоторых областях индустрии безопасность все еще не является приоритетам, и это может подвергнуть организации и их клиентов риску со стороны хакеров.

Компания по кибербезопасности Kela изучила подпольные форумы и обнаружила экосистему, основанную на покупке и продаже начального сетевого доступа игровым компаниям, а также выставленных на продажу почти одного миллиона скомпрометированных учетных записей игровых сотрудников и клиентов, причем половина из них была выставлена на продажу только в 2020 году.

Скомпрометированные учетные данные, выставленные на продажу - часто всего за несколько долларов - включают имена пользователей и пароли для всех видов бизнес-ресурсов, используемых сотрудниками игровых компаний, включая панели администратора, виртуальные частные сети, среды разработки, ресурсы для клиентов и многое другое.

Но в некоторых случаях киберпреступникам даже не нужно рыскать по подпольным форумам в поисках рекламы о продаже скомпрометированных учетных записей - исследователи говорят, что в результате предыдущих утечек данных доступно 500 000 утечек учетных данных.

К ним относятся то, что компания описала как «высокопоставленные адреса электронной почты, такие как адреса высокопоставленных сотрудников и адреса электронной почты, которые обычно являются важным каналом в компании», включая финансовую, кадровую и ИТ-поддержку.

Имея в руках такую информацию, кибер-злоумышленники могут получить доступ к более широкой сети - или даже к сетям других предприятий, которые являются частью цепочки поставок скомпрометированной цели.

Это могут быть атаки, предназначенные для сбора дополнительных учетных данных для дополнительного использования, или даже возможно, что скомпрометированные учетные данные могут использоваться для развертывания программ-вымогателей в сети.

Онлайн-игры могут быть прибыльным бизнесом, и киберпреступники знают это, поэтому наблюдается рост подпольной деятельности, направленной на нацеливание на эти предприятия: пользователи либо продают, либо запрашивают доступ к компаниям, занимающимся онлайн-играми, по всему миру в разной степени.

В одном случае исследователи отправили сообщение продавцу, который предлагал доступ к облачному хранилищу «крупного разработчика игр», и продавцы предложили доступ к этому ресурсу, а также «крупному японскому разработчику игр», предположив, что некоторые из хакеров в этом пространстве есть гораздо более широкий доступ к скомпрометированным компаниям, чем кажется на первый взгляд.

«Как мы все наблюдаем, атаки и злоумышленники становятся все более изощренными и настраиваются на жертву. Некоторые злоумышленники пытаются найти конкретные данные и информацию, которые имеют отношение к масштабам или отрасли жертвы, и воспроизвести успешные атаки, "исследователи сказали в сообщении блога.

Чтобы помочь компаниям, занимающимся онлайн-играми, не украсть учетные данные или не стать жертвами других кибератак, рекомендуется использовать уникальные пароли для сотрудников, чтобы они не использовали одни и те же пароли в двух местах, а это означает, что если их можно будет идентифицировать в другом случае пароль не будет работать с их корпоративной учетной записью.

Также рекомендуется, чтобы организации применяли политики многофакторной аутентификации по всему бизнесу, поэтому, если киберпреступники действительно получают доступ к корпоративным учетным данным для входа в систему, им гораздо сложнее получить доступ к сети и перемещаться по ней». ***(Danny Palmer. Cyber criminals are taking aim at online gaming for their next big pay day // ZDNet (https://www.zdnet.com/article/cyber-criminals-are-taking-aim-at-online-gaming-for-their-next-big-pay-day/). 06.01.2021).***

***

«Ho Mobile, итальянский оператор мобильной связи, принадлежащий Vodafone, подтвердил в понедельник массовую утечку данных и теперь предпринимает редкий шаг, предлагая заменить SIM-карты всех затронутых клиентов.

Считается, что от взлома пострадали примерно 2,5 миллиона клиентов.

Впервые об этом стало известно в прошлом месяце, 28 декабря, когда аналитик по безопасности заметил, что база данных телекоммуникационной компании выставлена на продажу на форуме в темной сети.

Хотя компания изначально преуменьшала значение этих первоначальных отчетов, Хо подтвердил инцидент в понедельник в сообщении, размещенном на ее официальном сайте, и в SMS-сообщениях, отправленных всем пострадавшим клиентам.

Заявление Хо подтверждает оценку исследователя безопасности о том, что хакеры взломали серверы Хо и украли данные о клиентах Хо, включая полные имена, номера телефонов, номера социального страхования, адреса электронной почты, даты и места рождения, национальность и домашние адреса.

Хотя в компании заявили, что при вторжении не было украдено никаких финансовых данных или сведений о звонках, Хо признал, что хакеры получили доступ к деталям, связанным с SIM-картами клиентов.

БЕСПЛАТНАЯ ЗАМЕНА SIM-КАРТЫ

Чтобы избежать даже малейшей угрозы телефонного мошенничества или атак с заменой SIM-карт, итальянская телекоммуникационная компания теперь предлагает замену SIM-карт всем пострадавшим клиентам, если они того пожелают, и бесплатно…

Поскольку SIM-карта и данные клиента были украдены и могут быть использованы для запроса смены SIM-карты, потребуется физическое присутствие в магазинах Но, заявила компания, чтобы не позволить хакерам запрашивать смену SIM-карты для законного клиента через Телефон.

Компания сообщила, что расследование взлома все еще продолжается вместе с местными правоохранительными органами.

В то время как нарушения безопасности имели место в различных телекоммуникационных компаниях по всему миру, это редкий случай, когда провайдер делает добро своим клиентам и предлагает бесплатную замену SIM-карты». ***(Catalin Cimpanu. Italian mobile operator offers to replace SIM cards after massive data breach // ZDNet (https://www.zdnet.com/article/italian-mobile-operator-offers-to-replace-sim-cards-after-massive-data-breach/). 05.01.2021).***

***

«Американский телекоммуникационный провайдер T-Mobile раскрыл на прошлой неделе нарушение безопасности, четвертое нарушение данных за последние три года после инцидентов в августе 2018 года, ноябре 2019 года и марте 2020 года.

«Наша команда по кибербезопасности недавно обнаружила и заблокировала вредоносный, несанкционированный доступ к некоторой информации, связанной с вашей учетной записью T-Mobile», - говорится в письмах компании, отправленных клиентам, полученных ZDNet, и на странице своего официального сайта.

T-Mobile заявила, что расследовала инцидент с помощью экспертов по кибербезопасности.

Расследование показало, что хакеры получали доступ к деталям клиентов, таким как номера телефонов, количество линий, подключенных к учетной записи, и, в некоторых случаях, к информации, связанной с вызовами, которую, по словам T-Mobile, она собирала в рамках нормальной работы своего беспроводного сервиса..

«Доступные данные не включают имена в учетной записи, физические адреса или адреса электронной почты, финансовые данные, информацию о кредитных картах, номера социального страхования, налоговый идентификатор, пароли или PIN-коды», - заявили в компании.

Поскольку никакая личная или финансовая информация не была раскрыта, T-Mobile не предоставляет бесплатные услуги кредитного мониторинга, а только уведомляет клиентов в соответствии с законами штата США.

Представитель T-Mobile сказал, что нарушение затронуло лишь 0,2% от общей пользовательской базы компании, что составляет около 200 000 человек.

Нарушение безопасности выглядит не так плохо, как предыдущие нарушения безопасности компании, в первую очередь из-за меньшего числа затронутых клиентов и менее конфиденциального характера открытых данных.

Эти предыдущие нарушения включают инцидент в марте 2020 года (когда T-Mobile заявила, что хакеры получили доступ как к данным его сотрудников, так и к клиентам, включая учетные записи электронной почты сотрудников), инцидент в ноябре 2019 года (когда T-Mobile заявила, что «обнаружила и отключила» несанкционированный доступ к личным данным своих клиентов) и инцидент в августе 2018 г. (когда T-Mobile заявила, что хакеры получили доступ к личным данным 2 миллионов его клиентов).

Перед слиянием с T-Mobile в 2020 году Sprint также обнаружил два нарушения безопасности в 2019 году: одно в мае, а второе - в июле». ***(Catalin Cimpanu. T-Mobile discloses its fourth data breach in three years // ZDNet (https://www.zdnet.com/article/t-mobile-discloses-its-fourth-data-breach-in-three-years/). 04.01.2021).***

***

«Операторы вредоносных программ, которые хотят знать местоположение зараженных ими жертв, обычно полагаются на простой метод, при котором они получают IP-адрес жертвы и сверяют его с базой данных IP-to-geo, такой как GeoIP MaxMind, чтобы получить приблизительное географическое местоположение жертвы.

Хотя этот метод не очень точен, он по-прежнему является наиболее надежным методом определения фактического физического местоположения пользователя на основе данных, обнаруженных на его компьютере.

Однако в своем блоге в прошлом месяце Ксавье Мертенс, исследователь безопасности из SANS Internet Storm Center, сказал, что он обнаружил новый штамм вредоносного ПО, использующий второй метод поверх первого.

Этот второй метод основан на получении BSSID зараженного пользователя.

BSSID, известный как «идентификатор базового набора услуг», в основном представляет собой физический MAC-адрес беспроводного маршрутизатора или точки доступа, которую пользователь использует для подключения через Wi-Fi.

Вы можете увидеть BSSID в системах Windows, выполнив команду:

netsh wlan показать интерфейсы | найти "BSSID"

Мертенс сказал, что обнаруженная им вредоносная программа собирала BSSID и затем проверяла его по бесплатной базе данных BSSID-to-geo, которую ведет Александр Мыльников.

Эта база данных представляет собой набор известных BSSID и последнего географического местоположения, в котором они были обнаружены.

Эти типы баз данных довольно распространены в наши дни и обычно используются операторами мобильных приложений в качестве альтернативных способов отслеживания пользователей, когда они не могут напрямую получить доступ к данным о местоположении телефона (например, см. WiGLE, одну из самых популярных служб, используемых для эти типы преобразования BSSID-to-geo).

Проверка BSSID по базе данных Мыльникова позволит вредоносному ПО эффективно определять физическое географическое местоположение точки доступа Wi-Fi, которую жертва использовала для доступа в Интернет, что является гораздо более точным способом определения географического положения жертвы.

Совместное использование обоих методов позволяет операторам вредоносных программ подтвердить правильность первоначального запроса геолокации по IP-адресу с помощью второго метода BSSID.

Операторы вредоносных программ обычно проверяют местонахождение жертвы, потому что некоторые группы хотят делать жертв только в определенных странах (например, в рамках операций, финансируемых государством) или они не хотят заражать жертв в своей стране (чтобы не привлекать внимание местных жителей). правоохранительные органы и избежание судебного преследования).

Однако базы данных IP-to-geo известны своими крайне неточными результатами, поскольку телекоммуникационные компании и центры обработки данных, как правило, приобретают или арендуют блоки IP-адресов на свободном рынке. Это приводит к тому, что некоторые IP-блоки назначаются различным организациям в других регионах земного шара от их первоначального / фактического владельца.

Использование второго метода для двойной проверки географического местоположения жертвы сегодня не является широко распространенным, но этот метод имеет очевидные преимущества, которые, несомненно, оценят другие вредоносные программы, которые решат использовать и в будущем». ***(Catalin Cimpanu. Malware uses WiFi BSSID for victim identification // ZDNet (https://www.zdnet.com/article/malware-uses-wifi-bssid-for-victim-identification/). 04.01.2021).***

***

«Ситуация с конфиденциальностью данных в Азии (Восток, Центр и Юг) и Тихоокеанском регионе претерпела драматические изменения за последнее десятилетие, и все указывает на то, что правила конфиденциальности в этом регионе будут продолжать меняться столь же быстрыми темпами в 2021 году и в последующий период. До 2010 года только шесть юрисдикций имели всеобъемлющие законы о конфиденциальности данных, и две из них приняли свои законы до 2000 года: Новая Зеландия в 1993 году и Гонконг в 1995 году. В период с 2010 по 2020 год еще 13 юрисдикций приняли новые законы о конфиденциальности данных, а семь внесли поправки в свои существующие законы (четыре из семи юрисдикций дважды вносили поправки в свои законы за этот 10-летний период).

В ближайшие пару лет мы можем увидеть восемь новых или обновленных законов, которые будут приняты или внесены в национальные законодательные органы. Китай, Индия и Индонезия, скорее всего, примут законы в краткосрочной перспективе, за ними следуют Австралия, Гонконг, Малайзия, Шри-Ланка и Вьетнам в более долгосрочной перспективе. Это означает, что одна треть существующих режимов конфиденциальности претерпит существенные изменения в ближайшие несколько лет.

Несмотря на то, что законы региона используют те же основные элементы защиты данных, которые присутствуют практически во всех законах о конфиденциальности в мире, каждый из них имеет свои собственные особые правила, которые отличаются друг от друга и от правил в других регионах. В отличие от ЕС, для этого региона характерны различные правовые системы и исторические различия, из-за которых невозможно сделать обобщение о законах Азии и Тихого океана. Эти различия важно учитывать при разработке глобальных или региональных программ соблюдения конфиденциальности. В этом предупреждении обсуждаются некоторые общие черты и различия между режимами конфиденциальности в регионе и определяются юрисдикции, которые могут принять новые или измененные законы в ближайшие несколько лет.

Характеристики современного регионального ландшафта: общие черты и различия

Девятнадцать юрисдикций в регионе теперь имеют всеобъемлющие законы о конфиденциальности. [1] Самые новые законы действуют в Таиланде [2] и Узбекистане. Недавно были внесены поправки в законы Японии, Казахстана, Кореи, Новой Зеландии и Сингапура. Хотя они используют одни и те же основные элементы защиты данных, все эти законы содержат определенные правила, которые отличаются друг от друга и от правил других регионов.

Объем. Большинство законов в этом регионе применяются только к обработке внутри страны. Однако пять имеют экстерриториальные положения, которые аналогичны экстерриториальным положениям Общего регламента ЕС по защите данных (GDPR) или превышают их: Австралия, Япония, Новая Зеландия, Филиппины и Таиланд.

Трансграничный. Точно так же три четверти (15) налагают ограничения на трансграничную передачу персональных данных. Однако на этом сходство заканчивается, потому что правовые основания для переводов варьируются от адекватности, согласия (или другой правовой основы, такой как юридические требования) и / или контактов (или обязательных корпоративных правил). Ни одна юрисдикция в регионе еще не выпустила список юрисдикций, обеспечивающих адекватную защиту, или, за исключением Новой Зеландии, типовые договорные положения. Более того, Новая Зеландия и Япония - единственные страны в регионе, которых ЕС считает адекватными. Южная Корея и Тайвань в настоящее время стремятся получить решение ЕС об адекватности.

Законы Гонконга, Индонезии, Непала и Тайваня не ограничивают трансграничную передачу личных данных.

Уведомление о нарушении. Немногим более половины (10) требуют уведомления в случае утечки данных. В то время как ряд законов требует, чтобы уведомление было направлено физическим лицам и / или органу по защите данных «незамедлительно» или «без промедления», другие законы требуют уведомления в течение 72 часов (Филиппины, Сингапур и Таиланд) или, в одном случае, в течении 14 дней.

Правовые основы обработки. Две трети законов (12) не разрешают обработку на основании законных интересов. Диапазон доступных правовых основ варьируется от одной юрисдикции к другой.

Индивидуальные права. Права доступа и исправления должны быть предоставлены во всех странах, кроме Непала. Почти половина законов (9) предоставляют права на удаление данных, но только четыре страны предоставляют права на переносимость данных: Китай (согласно Стандарту конфиденциальности), Филиппины, Сингапур и Таиланд. Сроки ответа на запросы о правах человека также сильно различаются: четыре страны требуют ответа на запросы о правах в течение 30 дней или более; два в течение 20–21 дня; два в течение 10–15 дней; и три в течение 1–7 дней. В семи не указан конкретный период времени.

Сотрудник по защите данных (DPO). Восемь законов требуют назначения DPO: Китай (согласно Стандарту конфиденциальности), Япония, Казахстан, Корея, Новая Зеландия, Филиппины, Сингапур и Таиланд.

Требования к локализации. Только две юрисдикции предъявляют требования к локализации данных: закон Казахстана о конфиденциальности требует от компаний хранить свои данные локально, а закон Китая о кибербезопасности требует от операторов критически важной инфраструктуры хранить в Китае как личную информацию, так и «важные данные», собираемые и производимые в ходе их деловых операций.

Регистрация. В то время как во всем мире наблюдается тенденция к минимизации требований к регистрации, пять законов в регионе требуют, чтобы организации регистрировали деятельность по обработке данных в органе по защите данных: Кыргызстан; Макао; Малайзия; Филиппины; и Узбекистан.

Оценка воздействия на защиту данных (DPIA). Большинство законов в регионе не требует от организаций проведения DPIA. DPIA требуются только в Сингапуре, Южной Корее и на Филиппинах.

Исполнение. После крупных утечек данных в регионе за последние несколько лет органы по защите данных (DPA) в Южной Корее, Японии и Австралии сосредоточили свое внимание на совершенствовании методов обеспечения безопасности частного сектора. DPA в Корее, Японии и Австралии были самыми агрессивными в проведении проверок и преследовании организаций, которые не применяли надлежащие меры безопасности, что часто приводило к штрафам и / или исправительным предписаниям.

Обеспечение соблюдения правил конфиденциальности в Китае, Гонконге и Сингапуре больше сосредоточено на других типах нарушений конфиденциальности.

Новые законы ожидаются в 2021 году и в последующий период

Индия. Внесен в законодательный орган Индии в 2019 г., Закон о защите личных данных, 2019 г.в настоящее время рассматривается Объединенным парламентским комитетом. Отчет комитета дважды задерживался из-за пандемии. Первоначально отчет был отложен до сессии парламента, посвященной сезонным дождям, которая проводится в период с июля по сентябрь, но эта сессия была прервана из-за пандемии. Затем ожидалось, что отчет будет выпущен во время зимней сессии, которая состоится в конце ноября / начале декабря, но эта сессия была полностью отменена из-за пандемии. Теперь кажется, что Парламент не может возобновить свою работу до бюджетной сессии Парламента, которая, как ожидается, состоится в январе 2021 года. Между тем появились противоречивые

сообщения о перспективах законопроекта. Член парламента Индии Раджив Чандрасекхар, В прессе сообщалось, что он выражает пессимизм в отношении его перспектив и заявляет, что не ожидает, что Объединенный парламентский комитет примет закон в его нынешнем виде. Напротив, министр связи и информационных технологий Рави Шанкар Прасад выразил оптимизм по поводу того, что закон будет доработан «очень скоро».

Учитывая пандемию и разногласия по поводу некоторых положений законопроекта, трудно сказать точно, когда и когда будет принят закон о конфиденциальности данных. В законопроекте есть ряд положений, вызывающих серьезную обеспокоенность отрасли, в частности, в отношении экстерриториальных положений предлагаемого закона, которые превышают положения GDPR, ограниченных правовых оснований для обработки персональных данных, ограничительных правил для перекрестных -граничная передача конфиденциальных и «важных» личных данных, обременительные обязательства по уведомлению о нарушениях, а также дополнительные и обременительные обязательства, налагаемые на определенные типы контроллеров данных и компании социальных сетей. Кроме того, законопроект предусматривает суровые наказания за нарушение закона, корпоративную ответственность и частные права на иск, включая коллективные иски. И, пожалуй, наиболее спорным и тревожным является положение в законопроекте, которое дает правительству право доступа к бизнес-аналитике и интеллектуальной собственности компаний для его собственных целей «планирования» и «развития». Некоторые из ключевых проблем с законодательством были изложены вматериалы, поданные Morrison & Foerster от имени Global Privacy Alliance.

Индонезия. В январе 2020 года правительство Индонезии внесло закон о конфиденциальности данных. В парламенте, и ожидается, что законопроект будет принят к концу года. Однако из-за пандемии ожидается, что законопроект будет доработан где-то в начале 2021 года. Если он будет принят в его нынешней форме, предложенный закон, среди прочего, потребует от контролеров обрабатывать персональные данные на основе согласия или на другом юридическом основании, таком как законные интересы или законное требование, для уведомления отдельных лиц и органа по защите данных в течение 72 часов после нарушения данных и для предоставления отдельным лицам прав доступа, исправления, удаления и переносимости данных. Кроме того, предложенный закон устанавливает ограничения на трансграничные переводы и запрещает покупку и продажу личных данных за деньги.

Китай. В октябре 2020 года правительство Китая выпустило проект закона о конфиденциальности после завершения 22-й сессии Постоянного комитета Тринадцатого Всекитайского собрания народных представителей. Проект закона о защите личной информации («Законопроект») был открыт для публичных обсуждений до 19 ноября 2020 года. Morrison & Foerster от имени Global Privacy Alliance подали комментарии в ходе этого разбирательства. На сегодняшний день в Китае не принят всеобъемлющий закон о защите данных, а приняты различные законы, постановления и необязательные стандарты, касающиеся безопасности и конфиденциальности данных, для конкретных секторов или проблем.

Среди прочего, Законопроект предусматривает узкий набор правовых основ для обработки личной информации, включая согласие, договорную необходимость и юридические требования, но не законные интересы. Законопроект также предъявляет требования к локализации данных операторам и контролерам критически важной информационной инфраструктуры, которые обрабатывают личную информацию в объеме, установленном Администрацией киберпространства Китая (CAC), требует уведомлений правительству в случае утечки данных, а также для Контроллеры, обрабатывающие личную информацию в количествах, предписанных CAC, требуют назначения сотрудника по защите данных. Штрафы за нарушения составляют до 50 миллионов йен (примерно 7,6 миллиона долларов США) или до 5% от оборота за предыдущий год. К тому же,

Ожидается, что закон может быть принят где-то в 2021 году.

Австралия. В октябре 2020 года правительство Австралии опубликовало для общественного обсуждения техническое задание и выпускает документ для всестороннего обзора Закона о конфиденциальности 1988 года (Закон о конфиденциальности). В настоящее время правительство изучает комментарии, полученные в ходе консультации, которая завершилась в конце ноября, а затем планирует выпустить в начале 2021 года дискуссионный документ, в котором будут запрашиваться более конкретные отзывы о предварительных результатах, включая любые возможные варианты реформы. Обзор охватывает такие области, как:

- объем и применение Закона о конфиденциальности;
- обеспечивает ли Закон о конфиденциальности эффективную защиту личной информации и обеспечивает ли практическую и соразмерную основу для продвижения надлежащей практики конфиденциальности;
- должны ли люди иметь прямые права на действия для обеспечения соблюдения обязательств в отношении конфиденциальности в соответствии с Законом о конфиденциальности;
- следует ли ввести в австралийское законодательство деликт по закону за серьезные посягательства на частную жизнь;
- влияние схемы утечки данных, подлежащей уведомлению, и ее эффективность в достижении поставленных целей;
- эффективность правоприменительных полномочий и механизмов в соответствии с Законом о конфиденциальности и их взаимодействие с другими нормативными базами Содружества; и
- желательность и осуществимость независимой схемы сертификации для мониторинга и демонстрации соблюдения австралийских законов о конфиденциальности.

Правительство работает над отдельным курсом, чтобы увеличить максимальные гражданские санкции в соответствии с Законом о конфиденциальности и разработать обязательный кодекс конфиденциальности для платформ социальных сетей и других онлайн-платформ, торгующих личной информацией.

Гонконг. Правительство Гонконга в настоящее время рассматривает и изучает возможные поправки к Постановлению о (конфиденциальности)

персональных данных (PDPO) Гонконга совместно с Управлением Уполномоченного по вопросам конфиденциальности персональных данных (PCPD). В рамках этого процесса Бюро по конституционным и материковым вопросам Гонконга выпустило дискуссионный документ. В январе 2020 года для выяснения мнения Группы Законодательного совета по конституционным вопросам о предлагаемых изменениях в НДПО. Возможные поправки включают расширение сферы действия закона (чтобы охватить процессоров и расширить определение персональных данных), наделение УКПБ полномочиями по уголовному расследованию и судебному преследованию, а также возможность назначать административные штрафы, повышение максимального уровня уголовных штрафов, введение обязательных данных нарушать обязательства по уведомлению и требовать от пользователей данных устанавливать политики хранения, определяющие максимальные сроки хранения для различных типов собираемых персональных данных.

Малайзия. В феврале 2020 года Департамент защиты персональных данных Малайзии («JPDP») провел общественные консультации по предлагаемым изменениям в Закон о защите персональных данных 2010 г. («Закон»). В консультативном документе на высоком уровне изложены возможные изменения Закона в 22 различных областях, включая уведомление о нарушениях, конфиденциальность по дизайну, переносимость данных и расширенную сферу действия для процессоров. Эта консультация последовала за годичным обзором, проведенным JPDP для сравнения Закона с другими международными законами о защите данных и изучения путей его усиления. Учитывая изменения в правительстве в 2020 году и пандемию, сроки разработки законопроекта неясны.

Шри-Ланка. Министерство цифровой инфраструктуры и информационных технологий Шри-Ланки выпустило проект текста закона о защите данных в сентябре 2019 года. В сентябре 2020 года сообщалось, что проект закона, как ожидается, будет представлен на утверждение кабинета министров. По заявлению министерства, закон вступит в силу в течение трех лет с даты его сертификации, чтобы предоставить государственному и частному сектору достаточно времени для принятия адекватных мер по соблюдению закона. Орган по защите данных необходимо создать в течение 18 месяцев.

Законопроект отражает GDPR во многих отношениях, таких как применимость закона, правовые основы для обработки, личные права, всеобъемлющие обязательства прозрачности и подотчетности для контроллеров (включая необходимость оценки воздействия на конфиденциальность) и запреты на отправку нежелательных маркетинговых сообщений. без явного согласия отдельных лиц. Кроме того, существуют требования к локализации данных для обработки персональных данных в государственном секторе.

Вьетнам. В октябре 2020 года правительство Вьетнама объявило, что оно поручило Министерству общественной безопасности (MPS) координировать свои действия с соответствующими министерствами, ведомствами и местностями для разработки и представления в первом квартале 2021 года проекта указа о защите персональных данных («Указ»). В июле 2020 года МОБ в сотрудничестве с Министерством юстиции и ООН провело семинар по защите данных, посвященный

малоимущим и уязвимым группам во Вьетнаме. Семинар проводился в рамках проекта «Программа ЕС по вопросам правосудия и расширения юридических прав во Вьетнаме» (EU JULE) в 2020 году для укрепления верховенства закона и доступа к правосудию. Ожидается, что результаты семинара будут использованы для разработки Указа и других соответствующих юридических документов, чтобы разработать правовую основу для защиты персональных данных во Вьетнаме». ***(Cynthia J. Rich. Transformation of the Privacy Landscape in Asia // Morrison & Foerster (https://www.mofo.com/resources/insights/210104-transformation-privacy-landscape-asia.html). 04.01.2021).***

***

«Резервный банк Новой Зеландии, известный как Te Pūtea Matua, пострадал от утечки данных после того, как злоумышленники взломали стороннего хостинг-партнера.

Резервный банк является центральным банком Новой Зеландии и отвечает за создание денежно-кредитной политики для стабилизации цен в стране.

10 января Резервный банк сообщил, что они пострадали от взлома данных после того, как злоумышленники незаконно получили доступ к данным, хранящимся у стороннего хостинг-провайдера.

«Сторонний сервис обмена файлами, используемый Банком для обмена и хранения конфиденциальной информации, подвергся незаконному доступу», - говорится в уведомлении.

Управляющий Резервного банка Адриан Орр заявляет, что нарушение было локализовано, но, возможно, раскрыла коммерческую и личную конфиденциальную информацию.

«Мы тесно сотрудничаем с отечественными и международными экспертами по кибербезопасности и другими соответствующими органами в рамках нашего расследования и реагирования на эту злонамеренную атаку. Характер и объем информации, к которой потенциально возможен доступ, все еще определяется, но она может включать в себя некоторую коммерческую и личную конфиденциальную информацию».

«Система была защищена и отключена до тех пор, пока мы не завершим наши первоначальные исследования. Чтобы понять все последствия этого нарушения, потребуется время, и мы работаем с пользователями системы, к информации которых мог быть получен доступ. Наши основные функции остаются надежными и работоспособными», - говорится в заявлении Орр…». ***(Lawrence Abrams. New Zealand Reserve Bank suffers data breach via hacked storage partner // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-zealand-reserve-bank-suffers-data-breach-via-hacked-storage-partner/). 10.01.2021).***

***

«Компания Dassault Falcon Jet выявила утечку данных, которая могла привести к раскрытию личной информации, принадлежащей нынешним и бывшим сотрудникам, а также их супругам и иждивенцам.

Dassault Falcon Jet - американская дочерняя компания французской аэрокосмической компании Dassault Aviation, которая проектирует и производит военные самолеты, бизнес-джеты и космические системы.

В дочерней компании Dassault работает 2453 сотрудника, и она специализируется на маркетинге и предоставлении авиационных услуг и услуг по техническому обслуживанию самолетов Falcon на американском континенте.

Выручка Dassault Aviation в 2019 году составила 7,3 миллиарда евро, и она поставила более 10 000 военных и гражданских самолетов в более чем 90 стран.

Дочерние компании также затронули

Компания Dassault Falcon Jet обнаружила инцидент 6 декабря 2020 года и 31 декабря отправила письмо с уведомлением об утечке данных затронутым нынешним и бывшим сотрудникам.

Согласно сообщениям СМИ и датам взлома, о которых сообщает компания, злоумышленники сохраняли доступ к системам Dassault Falcon Jet в течение примерно шести месяцев, с 6 июня по 7 декабря.

Операторы Ragnar Locker, проникшие в системы компании, также смогли проникнуть в сеть нескольких дочерних компаний Dassault Falcon Jet.

В основные дочерние компании включают в себя Dassault Aircraft Services Corporation, Aero Precision и капитальный ремонт компании (Apro), Midway авиастроительной корпорации Instrument, Dassault Falcon Jet Do Brasil LIMITADA и Dassault Falcon Jet Лизинг.

«После обнаружения этого инцидента безопасности мы немедленно отключили все затронутые системы и привлекли сторонних экспертов по кибербезопасности для помощи в нашем расследовании, поскольку мы работаем над безопасным восстановлением наших систем таким образом, чтобы защитить безопасность вашей информации», - нарушение уведомление говорит.

Компания сотрудничает с правоохранительными органами для расследования инцидента и заявляет, что нашла доказательства того, что злоумышленники могли украсть документы, содержащие информацию о сотрудниках.

Информация, принадлежащая сотрудникам, может включать их «имя, личный и корпоративный адрес электронной почты, личный почтовый адрес, идентификационный номер сотрудника, номер водительских прав, паспортные данные, номер финансового счета, номер социального страхования, дату рождения, место работы, компенсацию и льготы. информация о зачислении и дате приема на работу».

Информация об их супругах и иждивенцах может включать их «имя, адрес, дату рождения, номер социального страхования и информацию о регистрации на пособие».

Затронутые системы восстановлены и перестроены

Хотя компания еще не подтвердила, что взлом был вызван атакой вымогателя, в декабре LeMagIT сообщил, что Ragnar Locker - это банда вымогателей, которая стояла за этим инцидентом.

Представители Dassault Falcon Jet не были доступны для комментариев, когда с ними связались сегодня представители BleepingComputer.

Компания также не ответила на запросы, сделанные BleepingComputer в прошлом месяце.

Однако в уведомлении о нарушении говорится, что затронутые системы были восстановлены и перестроены после инцидента.

«По мере того, как мы восстанавливаем и перестраиваем системы, мы также усиливаем меры безопасности, чтобы защитить эти системы и данные, хранящиеся на них», - заявили в компании…». ***(Sergiu Gatlan. Dassault Falcon Jet reports data breach after ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/dassault-falcon-jet-reports-data-breach-after-ransomware-attack/). 08.01.2021).***

***

«Хакер продает данные, украденные у гиганта по производству каннабиса Aurora Cannabis после взлома их систем в рождественский день.

Aurora Cannabis - канадский производитель каннабиса, котирующийся на фондовой бирже Торонто и Нью-Йоркской фондовой бирже. Компания управляет многочисленными медицинскими и потребительскими брендами, связанными с каннабисом, включая MedRelease, CanniMed, Whistler Medical Marijuana Corp., San Rafael, Daily Special и Woodstock.

Marijuana Business Daily сообщила, что бывшие и нынешние сотрудники получили уведомления об утечке данных от Aurora Cannabis после того, как компания пострадала от кибератаки 25 декабря 2020 года.

Уведомления об утечке данных описывают, какие данные были украдены в результате атаки, при этом каждый сотрудник сообщает о разных скомпрометированных данных.

«Он сказал, что каждый человек сообщил о разных данных, скомпрометированных в результате взлома, включая информацию о кредитной карте, официальные документы, домашний адрес и банковские реквизиты», - сообщает MBD.

Хакер продает украденные данные за один биткойн

Сегодня хакер, стоящий за атакой Aurora Cannabis, начал продавать украденные данные на хакерском форуме за один биткойн, примерно 39000 по сегодняшним ценам. В рамках сообщения, рекламирующего продажу, злоумышленник опубликовал изображения одиннадцати файлов, украденных во время атаки.

Образцы украденных данных включали изображения паспортов, чеков, водительских прав и деловых документов.

В интервью хакеру BleepingComputer сообщили, что 25 декабря Aurora Cannabis была взломана после того, как злоумышленник взломал их сеть.

Злоумышленник утверждает, что украл 50 ГБ данных, включая личные данные клиентов и сотрудников.

После кражи данных хакер заявляет, что они связались с Aurora Cannabis, чтобы выкупить данные, но «все они игнорируют это нарушение».

Злоумышленник утверждает, что у них все еще есть доступ к сети Авроры. Когда его спросили, знает ли Аврора, что у них по-прежнему есть доступ,

BleepingComputer ответили: «Я отправляю почту, но думаю, что все сотрудники меня игнорировали».

BleepingComputer связался с Aurora Cannabis по поводу атаки, но не получил ответа». ***(Lawrence Abrams. Hacker sells Aurora Cannabis files stolen in Christmas cyberattack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hacker-sells-aurora-cannabis-files-stolen-in-christmas-cyberattack/). 07.01.2021).***

***

«На этой неделе на компанию Canon USA Inc. (Canon) был подан коллективный иск в окружном суде Восточного округа Нью-Йорка в связи с атакой программы-вымогателя, в результате которой в ноябре 2020 года были раскрыты личные данные нынешних и бывших сотрудников., Нью-Йорк, Флорида и Иллинойс, и утверждают, что компания Canon небрежно защищала данные сотрудников и нарушила законы штата о торговой практике, не приняв мер защиты от такой атаки. Истцы также утверждают, что Canon не вовремя уведомила пострадавших лиц.

Атака на Cannon произошла в августе 2020 года и затронула нынешних и бывших сотрудников с 2005 по 2020 год, а также их бенефициаров и иждивенцев. Затронутая информация включала номера социального страхования, номера водительских прав, номера финансовых счетов, электронные подписи и даты рождения. Истцы добиваются сертификации общенационального класса». ***(KATHRYN RATTIGAN. Canon Hit with Data Breach Class Action Suit by Former and Current Employees // Robinson+Cole LLP. (https://www.dataprivacyandsecurityinsider.com/2021/01/canon-hit-with-data-breach-class-action-suit-by-former-and-current-employees/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+DataPrivacyAndSecurityInsider+%28Data+Privacy+%2B+Security+Insider%29). 07.01.2021).***

***

«Данные о пациентах Apex Laboratory были опубликованы и размещены на сайте утечки.

Лаборатория Apex, которая предоставляет анализы крови на дому для пациентов в Нью-Йорке, Лонг-Айленде и Южной Флориде, подверглась атаке с использованием программ-вымогателей, в результате которой были украдены данные пациентов.

Хотя компания только что сообщила об атаке, она произошла 25 июля, когда «определенные системы в ее среде были зашифрованы и недоступны», согласно сообщению веб-сайта от прошлой недели.

Работая с фирмой, занимающейся кибербезопасностью, Apex смогла защитить свою сеть и возобновить работу через два дня. Но судебно-медицинское расследование продолжалось, и в конечном итоге 15 декабря было установлено, что злоумышленники разместили в своем блоге информацию об атаке и

утверждали, что утащили личную и медицинскую информацию, сообщила компания в новогоднем уведомлении.

Эти данные включают имена пациентов, даты рождения, результаты тестов, а для некоторых людей - номера социального страхования и номера телефонов, сообщает Apex. Скорее всего, он был взят из систем Apex в период с 21 по 25 июля в рамках атаки с «двойным вымогательством», когда преступники не только блокируют системы, но и захватывают данные.

«Apex не знает о фактическом или попытках неправомерного использования какой-либо информации, кроме извлечения этих данных в рамках кибератаки», - заявили в компании. «Apex находится в процессе подготовки письменного уведомления по почте для пострадавших лиц, для которых у него есть адреса». Он добавил, что расследование все еще продолжается.

«В то время как типичная бизнес-модель программ-вымогателей включает шифрование данных на месте с последующей продажей возможностей дешифрования жертвы (также известных как выкуп), бизнес-модели всегда развиваются», - сказал Threatpost Оливер Таваколи, технический директор Vectra. «Чтобы максимально увеличить вероятность того, что намеченная организация заплатит такой выкуп, злоумышленники могут решить причинить несколько видов боли - в этом случае злоумышленники использовали как возможную потерю данных через шифрование, так и публичное раскрытие конфиденциальной информации. информацию, тем самым получив два укуса яблока. В то время как у Apex Laboratory было достаточно хороших резервных копий данных, чтобы преодолеть первую угрозу, вторая угроза заключалась в том, что злоумышленник все же смог получить выкуп».

Другие подробности атаки были скудными, но Threatpost обратился к Apex за дополнительной информацией о причастной к атаке банде вымогателей и другими данными.

Новости поступают, поскольку медицинские организации продолжают оставаться главной мишенью для банд вымогателей,

«Я бы сказал, что сейчас основная проблема, с которой сталкивается здравоохранение, - это программы-вымогатели», - сказал Threatpost в интервью Threatpost в недавнее видео - интервью. «Программы-вымогатели продолжают оставаться главной проблемой при оказании медицинской помощи, поскольку они могут оказывать помощь пациентам. приходит программа-вымогатель и останавливает клинические операции, она может вызвать переадресацию ухода за пациентами, в результате чего они в основном отправляют машины скорой помощи в другие больницы или даже заставляют больницы переводить пациентов в другое учреждение, на которое не распространяется программа-вымогатель».

По словам исследователей, медицинские организации сталкиваются с уникальным набором проблем, которые делают их зрелыми мишенями.

«Отрасль здравоохранения имеет особенно сложные условия - они должны уделять первоочередное внимание борьбе с пожарами, связанными со здравоохранением, и должны работать с программным обеспечением (и оборудованием), на сертификацию безопасности которого уходят годы», - сказал Мохит Тивари, соучредитель и генеральный директор компании Компания

Symmetry Systems сообщила Threatpost. «Это означает, что вычислительная инфраструктура отстает как по коммерческим, так и по техническим причинам. Руководители здравоохранения нуждаются в изменении мышления. Они должны понимать, что вычислительная инфраструктура в больницах является ключом к здравоохранению, а сбои вычислений - это сбои здравоохранения. Кроме того, вычислительные недостатки тесно взаимосвязаны и могут быстро распространяться - программы-вымогатели или взлом больших хранилищ данных - или компрометация медицинского оборудования в сети». ***(Tara Seals. Ransomware Gang Collects Data from Blood Testing Lab // Threatpost (https://threatpost.com/ransomware-gang-data-blood-testing-lab/162721/). 04.01.2021).***

***

«Представители компании сказали, что начиная с июня, неизвестные имели несанкционированный доступ к серверам и могли скомпрометировать данные клиентов.

Исходя из информации от Kawasaki, впервые несанкционированный доступ к серверу в Японии был замечен 11 июня 2020 года из Тайланда. После закрытия доступа злоумышленникам произошло ещё несколько подобных инцидентов. Злоумышленники атаковали сервер из Индонезии, Филиппин и США.

Как заявил представитель компании, некоторая информация могла утечь к третьим лицам. Однако до сих пор свидетельств утечки не было обнаружено. На данный момент компания связывается с клиентами, которые могли быть вовлечены в инцидент». ***(Японская аэрокосмическая компания Kawasaki предупредила об утечке данных // SecureNews (https://securenews.ru/japanese-aerospace-company-kawasaki-warns-of-data-breach/). 04.01.2021).***

***

«Facebook подал сегодня в Португалии иск против двух граждан Португалии за разработку расширений для браузеров, которые собирали данные пользователей с сайтов Facebook.

«Когда люди устанавливали эти расширения в свои браузеры, они устанавливали скрытый код, предназначенный для считывания их информации с веб-сайта Facebook, а также информации из браузеров пользователей, не связанной с Facebook, - и все это без их ведома», - Джессика Ромеро, директор по платформе Facebook Правоприменение и судебные разбирательства, сказал сегодня.

«Если пользователь посещал веб-сайт Facebook, расширения браузера были запрограммированы на очистку его имени, идентификатора пользователя, пола, статуса отношений, возрастной группы и другой информации, связанной с его учетной записью», - сказал Ромеро.

Все расширения были разработаны компанией-разработчиком программного обеспечения под названием "Oink and Stuff", специализирующейся на создании приложений для Android и расширений браузеров для Chrome, Firefox, Opera и Microsoft Edge.

В то время как компания разрабатывает широкий спектр расширений для браузера, Facebook заявила, что обнаружила вредоносное поведение, связанное со

сбором данных, внутри четырех расширений, названных Web for Instagram plus DM, Blue Messenger, Emoji keyboard и Green Messenger, которые, по словам Facebook, «работали как шпионское ПО».

Все четыре расширения все еще доступны в официальном Интернет-магазине Chrome на момент написания, и их в сумме установили более 54 000 раз.

Facebook теперь просит португальского судью наложить постоянный судебный запрет на команду Oink and Stuff и заставить компанию удалить все данные пользователей Facebook, которые они получили с помощью четырех расширений.

Запрос на комментарий был отправлен в Oink and Stuff, но компания не ответила до публикации этой статьи из-за разницы в часовых поясах…» ***(Catalin Cimpanu. Facebook sues two Chrome extension devs for scraping user data // ZDNet (https://www.zdnet.com/article/facebook-sues-two-chrome-extension-devs-for-scraping-user-data/). 14.01.2021).***

***

«Mimecast, компания, которая производит облачное программное обеспечение для управления электронной почтой, сегодня раскрыла инцидент безопасности, предупредив клиентов, что «изощренный злоумышленник» получил один из ее цифровых сертификатов и злоупотребил им, чтобы получить доступ к некоторым учетным записям Microsoft 365 своих клиентов.

Лондонская компания, занимающаяся разработкой программного обеспечения для электронной почты, заявила, что данный сертификат использовался в нескольких ее продуктах для подключения к инфраструктуре Microsoft.

Продукты, которые использовали этот сертификат, включают продукты Mimecast Sync and Recover, Continuity Monitor и IEP, говорится в сообщении компании, опубликованном сегодня на ее веб-сайте.

Mimecast сообщила, что около 10% всех ее клиентов использовали затронутые продукты с этим конкретным сертификатом; однако «изощренный злоумышленник» злоупотребил украденным сертификатом, чтобы получить доступ только к небольшому количеству учетных записей Microsoft 365 этих клиентов.

Поставщик программного обеспечения электронной почты назвал это число ниже 10, описав его как «низкое однозначное число», и сказал, что он уже связался со всеми затронутыми клиентами.

Чтобы предотвратить злоупотребления в будущем, компания теперь просит всех других клиентов «немедленно удалить существующее соединение в своем клиенте M365 и повторно установить новое соединение на основе сертификата, используя новый сертификат, который [они] сделали доступным».

Mimecast заявила, что теперь работает со сторонним экспертом по криминалистике, Microsoft и правоохранительными органами, чтобы расследовать, как сертификат был скомпрометирован, и его последствия.

Лондонская компания заявила, что узнала об инциденте от Microsoft после того, как технический гигант обнаружил несанкционированный доступ к некоторым учетным записям.

Представитель Mimecast не стал комментировать, был ли инцидент каким-либо образом связан с недавней атакой на цепочку поставок SolarWinds». ***(Catalin Cimpanu. Mimecast says hackers abused one of its certificates to access Microsoft accounts // ZDNet (https://www.zdnet.com/article/mimecast-says-hackers-abused-one-of-its-certificates-to-access-microsoft-accounts/). 12.01.2021).***

***

«Производитель сетевых устройств Ubiquiti объявила об инциденте, связанном с безопасностью, в результате которого были раскрыты данные его клиентов.

Ubiquiti - очень популярный производитель сетевых устройств, наиболее известный своей линейкой проводных и беспроводных сетевых продуктов UniFi и платформой управления облаком.

Сегодня Ubiquiti начала отправлять клиентам электронные письма с просьбой изменить их пароли и включить 2FA после того, как злоумышленник взломал их системы, размещенные у стороннего поставщика облачных услуг.

«Недавно нам стало известно о несанкционированном доступе к некоторым нашим системам информационных технологий, размещенным сторонним поставщиком облачных услуг. У нас нет никаких свидетельств того, что имела место несанкционированная активность в отношении учетной записи любого пользователя», - написала Ubiquiti клиентам по электронной почте.

Ubiquiti заявляет, что им ничего не известно о клиентских базах данных, к которым был осуществлен незаконный доступ, но они не могут быть уверены, что атака не раскрыла данные клиентов.

"В настоящее время нам не известны доказательства доступа к каким-либо базам данных, в которых хранятся пользовательские данные, но мы не можем быть уверены в том, что пользовательские данные не были раскрыты. Эти данные могут включать ваше имя, адрес электронной почты и односторонний зашифрованный пароль для вашего (с технической точки зрения пароли хешируются и обрабатываются). Данные могут также включать ваш адрес и номер телефона, если вы предоставили их нам», - продолжалось в электронном письме…

Владельцы Ubiquiti разочарованы тем, что UniFi требует от них создания облачных учетных записей для управления локальными устройствами, и многие предпочли бы иметь возможность управлять всем локально.

В минувшие выходные в Ubiquiti произошел массовый сбой в работе своей платформы управления облаком UniFi, из-за которой пользователи не могли использовать веб-сайты и мобильные приложения или управлять своими устройствами.

Неизвестно, связано ли это отключение с инцидентом безопасности, раскрытым сегодня…». ***(Lawrence Abrams. Networking giant Ubiquiti alerts customers of potential data breach // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/networking-giant-ubiquiti-alerts-customers-of-potential-data-breach/). 11.01.2021).***

***

«Хакеры подсадили кейлоггер на сайт NZBGeek, популярный ресурс для индексации пиратского контента в Usenet, а также скопировали его базу данных с именами пользователей и зашифрованными паролями.

40-летняя сеть

Популярный сайт в сети Usenet NZBGeek пал жертвой кибератаки, в результате которой злоумышленники сумели завладеть солидным количеством пользовательских данных, в том числе информацией о кредитных картах.

Usenet — одна из самых старых сетей, предтеча современных интернет-форумов, запущенная еще в 1980 г. Несмотря ни на что, она существует и пользуется некоторой популярностью и по сей день, хотя, например, еще в 2008 г. Slashdot объявлял о ее кончине.

Впрочем, довольно значительная часть ее ресурсов сегодня используется для распространения пиратского контента — в качестве альтернативы BitTorrent.

Подробности взлома

NZBGeek был создан в 2012 г. в качестве платного сервиса для индексации веток с любым контентом, включая пиратский.

27 декабря 2020 г. стало известно о хакерской атаке, в результате которой злоумышленникам достались пользовательские имена, зашифрованные пароли, адреса электронной почты и номера кредитных карт. Операторы сайта заявили, что где-то в районе 20 ноября злоумышленники с помощью SQL-эксплойта подсадили на сайт кейлоггер на базе Javascript, так что под угрозой оказались все пользователи, заходившие на сайт после этого.

Именно кейлоггер позволил перехватывать данные о кредитных картах — на самом сайте они, по утверждению операторов NZBGeek, не хранятся.

Кроме того, хакерам удалось скопировать всю базу данных, в которой хранились, пусть и в зашифрованном виде, пароли, а также пользовательские имена, адреса электронной почты и последние IP-адреса, с которых пользователи обращались к сайту.

По словам операторов сайта, в момента атаки вышел из строя жесткий диск системы, через которую производилась индексация ресурсов в Usenet и API-сервер сайта.

Пользователям NZBGeek рекомендовано принять меры по защите своих кредитных карт от мошеннических транзакций.

«Улов достаточно богат, чтобы с помощью этих данных нанести вполне реальный финансовый ущерб пользователям взломанного сайта, что бы он собой ни представлял, — полагает Анастасия Мельникова, эксперт по информационной безопасности компании SECConsultServices. — Пострадают главным образом те, кто использовал одни и те же пароли на разных ресурсах. Сопоставить пользовательские имена с данными из прежних утечек очень простая задача». ***(Роман Георгиев. Сайт в древней, но живучей всемирной сети пал жертвой взлома // CNews (https://safe.cnews.ru/news/top/2021-01-11_sajt_v_drevnejno_zhivuchej). 11.01.2021).***

***

«Закон Калифорнии о правах на неприкосновенность частной жизни («CPRA») совершает прорыв в области кибербезопасности, внося поправки в Закон Калифорнии о конфиденциальности потребителей («CCPA»), предусматривающие усиление защиты. Усовершенствования CPRA применяются к «коммерческим» компаниям и другим организациям: (а) с валовой выручкой более 25 миллионов долларов в предыдущем календарном году или (б) которые ежегодно покупают, продают или делятся личной информацией 100 000 или более потребителей. или домохозяйства, или (с) которые получают не менее 50 процентов своего годового дохода от продажи или обмена личной информацией потребителей («бизнес»). [1] Эти компании должны:

- обеспечивать разумные гарантии кибербезопасности для всех категорий личной информации;
- проводить ежегодные аудиты кибербезопасности и подавать нормативные документы по оценке рисков в недавно созданное Калифорнийское агентство по защите конфиденциальности, если обработка личной информации представляет значительный риск для конфиденциальности или безопасности потребителей; и
- требуют договорных положений и других мер безопасности для устранения рисков безопасности и конфиденциальности цепочки поставок, когда они передают, делятся или иным образом раскрывают личную информацию своим поставщикам и другим третьим сторонам.

CPRA также:

- налагает ответственность за нарушение в соответствии с частным правом на иск и установленным законом возмещением ущерба за неспособность разумно защитить электронную почту человека в сочетании с паролем или секретным вопросом и ответом, разрешающим доступ к онлайн-аккаунту (например, учетные данные для входа); и
- устраняет 30-дневные безопасные гавани для организаций, пытающихся постфактум обезопасить себя от установленных законом убытков или штрафов путем внедрения мер защиты кибербезопасности после утечки данных или после уведомления о несоблюдении.

CPRA вступает в силу 1 января 2023 года, за исключением запросов потребителей на доступ к своим данным, которые будут «оглядываться» на данные, собранные бизнесом не ранее, чем 1 января 2022 года. [2] Предприятиям следует запланировать выполнение этих повышенных требований прямо сейчас, поскольку эффективное внедрение операционных и договорных процессов потребует значительного времени на выполнение заказа (так же, как и при переходе к дате вступления в силу 25 мая 2018 г. требований Общего регламента ЕС по защите данных («GDPR»)). Одним из важных соображений для предприятий является то, как они будут соответствовать этим новым требованиям безопасности в связи с внутренними и сторонними системами, службами и приложениями, собирающими или обрабатывающими личные данные жителей Калифорнии, помимо номеров социального страхования, номеров кредитных / дебетовых карт и аналогичных частных данные. Поправки повлияют на обязанности сотрудников, ответственных за разработку продуктов, технологий и услуг для клиентов или кто иным образом обрабатывает индивидуально идентифицируемую информацию о клиентах, а также

специалисты в области информационных технологий и аудиторы, отвечающие за кибербезопасность. Розничная торговля, гостиничный бизнес, интернет и другие предприятия, которые широко собирают личную информацию своих клиентов из Калифорнии, будут среди предприятий, на которые повлияют новые требования к кибербезопасности.

Разумное требование защиты для всех категорий личной информации : обязательство по внедрению разумных мер защиты кибербезопасности прямо расширяется в соответствии с CPRA за пределы текущего обязательства по защите номеров социального страхования и другой частной информации (например, номеров водительских прав, других государственных идентификаторов и медицинских, биометрическая и другая информация, определенная в соответствии с §1798.81.5 Cal. Civ. Code) для включения всех категорий личной информации. CPRA требует, чтобы компании «принимали разумные меры предосторожности для защиты личной информации потребителей от взлома». CPRA §B (6). CPRA также прямо требует в качестве утвердительного «обязательства», чтобы компания, которая «собирает личную информацию потребителя, применяла разумные процедуры и методы безопасности, соответствующие характеру личной информации, для защиты личной информации от несанкционированного или незаконного доступа, уничтожения, использования., изменение или раскрытие в соответствии с Разделом 1798.81.5.» CPRA §1798.100 (e). Компаниям необходимо будет подумать о том, как разумно защитить любую индивидуально идентифицируемую информацию, которая в соответствии с широким определением CCPA идентифицирует, относится к: описывает или разумно может быть связан или мог быть связан, прямо или косвенно, с конкретным лицом или домохозяйством. Cal. Civ. Кодекс §1798.140 (o) (1). Включение CPRABce категории личной информации в соответствии с явным положительным обязательством по внедрению разумных мер защиты кибербезопасности приводят Калифорнию в соответствие с требованиями GDPR EC, предусматривающими соответствующие меры безопасности, основанные на рисках, для всех личных данных. Расширенный охват потребует от предприятий определения всех категорий личной информации, собираемой или обрабатываемой для своих клиентов, информационных систем, которые собирают или обрабатывают этот более широкий объем данных, персонала, который обрабатывает эти процессы, и определения необходимых разумных мер безопасности на основе рисков. для защиты информации от несанкционированного доступа и других угроз безопасности.

Оценка рисков и аудиты кибербезопасности, необходимые для предприятий, чьи методы обработки данных представляют «значительный риск» для конфиденциальности или безопасности потребителей : CPRA предусматривает выпуск правил, требующих проведения ежегодного аудита кибербезопасности (на дату вступления в силу) теми предприятиями, чьи данные обработка представляет собой «значительный риск» для конфиденциальности или безопасности, «включая определение объема аудита и создание процесса, обеспечивающего тщательный и независимый аудит.. » CPRA § 1798.185 (a) (15) (A) (курсив добавлен). CPRA предусматривает правила, в которых перечисляются «факторы, которые

необходимо учитывать при определении того, когда обработка может привести к значительному риску для безопасности личной информации [и] должна включать размер и сложность бизнеса, а также характер и объем операций по обработке.” Как минимум, предприятия, которые собирают «конфиденциальную личную информацию» в соответствии с новым определением CPRA, могут подпадать под требования аудита из-за предсказуемых неблагоприятных последствий нарушения. «Конфиденциальная личная информация» означает: (A) социальное обеспечение потребителя, водительские права, государственное удостоверение личности или номер паспорта; (B) вход в учетную запись потребителя, финансовый счет, дебетовую карту или номер кредитной карты в сочетании с любым необходимым кодом безопасности или кодом доступа, паролем, или учетные данные, позволяющие получить доступ к учетной записи; (C) точное местоположение потребителя; (D) расовое или этническое происхождение, религиозные или философские убеждения потребителя или членство в профсоюзе; (E) содержание почты, электронной почты и текстовых сообщений потребителя, если только компания не является предполагаемым получателем сообщения; (F) генетические данные потребителя; и (2) (A) обработка биометрической информации с целью однозначной идентификации потребителя; (B) собираемая и анализируемая личная информация о здоровье потребителя; или (C) собранная и проанализированная личная информация о сексуальной жизни или сексуальной ориентации потребителя». CPRA §1798.140 (к.в.). Требование «независимого» и «тщательного» аудита является значительной гарантией. Какие бы подробности ни были устранены будущими правилами,

CPRA также требует, чтобы бизнес, участвующий в такой обработке «значительного риска», подпадал под действие правил, требующих подачи в Калифорнийское агентство по защите конфиденциальности «на регулярной основе оценки рисков в отношении обработки ими личной информации, включая вопрос о том, связана ли обработка с конфиденциальной информацией. персональной информации, а также выявление и взвешивание выгод, получаемых от обработки для бизнеса, потребителя, других заинтересованных сторон и общественности, с потенциальными рисками для прав потребителя, связанными с такой обработкой, с целью ограничения или запрещения такой обработки. обработка, если риски для конфиденциальности потребителя перевешивают выгоды от обработки для потребителя, бизнеса, других заинтересованных сторон и общественности». CPRA § 1798.185 (a) (15) (B). Закон штата Нью-Йорк SHIELD и HIPAA. Однако требование о том, чтобы фактическая оценка риска подлежала упорядоченной государственной регистрации и надзору со стороны регулирующих органов, является важным событием. Организации должны начать сейчас определять свои действия по обработке более высокого риска и учитывать достаточность своих оценок рисков, связанных с этими методами, с использованием обоснованной структуры оценки рисков (например, NIST).

Договорные и другие гарантии, необходимые для обмена личной информацией с третьими сторонами : бизнес должен включать, среди прочего,в своих контрактах с третьими сторонами, поставщиками услуг или подрядчиками, с которыми она делится личной информацией, о том, что принимающая сторона (i)

соблюдает «применимые обязательства в соответствии с этим заголовком» (включая разумные гарантии), (ii) «обязывает этих лиц предоставлять тот же уровень защиты конфиденциальности, который требуется этим заголовком », и (iii) предоставить бизнесу право принимать разумные меры для прекращения и устранения несанкционированного использования. CPRA §1798.100 (d). Кроме того, контракт должен включать требование о том, чтобы третья сторона, поставщик услуг или подрядчик уведомляла бизнес, если он определит, что он «больше не может выполнять свои обязательства» по соблюдению обязательств по обеспечению конфиденциальности и кибербезопасности. Это последнее требование отражает недавние инструкции GDPR в отношении трансграничной передачи данных. включая использование договорных гарантий для импортера данных для своевременного заблаговременного уведомления экспортера данных о его неспособности соблюдать свои договорные обязательства и обеспечить «практически эквивалентный уровень защиты данных». Компании, которые раскрывают или передают личную информацию другим организациям, должны сейчас начать изучать эти договорные соглашения и рассматривать изменения или дополнения. Эти соглашения, например, могут продлеваться до даты вступления в силу 1 января 2023 г., но применяться к данным, собранным или обработанным на дату вступления в силу или после нее, или регулировать методы обработки данных после 1 января 2022 г., которые могут быть доступны в будущем для потребителей. запрос.

Расширенная ответственность за нарушение и устранение 30-дневных периодов исправления: теперь CPRA предусматривает частное право на иск и установленный законом минимальный ущерб за несанкционированный доступ и кражу, кражу или раскрытие информации для входа в систему в результате нарушения предприятием обязанность внедрять и поддерживать разумные методы кибербезопасности. CPRA § 1798.150 (a) (1). [3] Более того, для любого нарушения, связанного с частным правом на иск, CPRA предусматривает, что «внедрение и поддержание разумных процедур и методов обеспечения безопасности в соответствии с Разделом 1798.81.5 в течение 30 дней после уведомления о нарушении не является лекарством от этого нарушения». CPRA § 1798.150 (b) (курсив наш). Нарушения, которые не привели к нарушению, могут быть исправлены в течение 30-дневного периода уведомления. CPRA § 1798.150 (b). Аналогичным образом, положение CCPA, предусматривающее, что компания может избежать нарушения и административных штрафов, если оно устраняет любое предполагаемое нарушение в течение 30 дней после уведомления о любом предполагаемом несоблюдении, было устранено. CPRA §1798.155. В будущих судебных процессах и административных правоприменительных действиях особое внимание будет уделяться позитивному обязательству CPRA по обеспечению превентивных разумных гарантий для всех категорий личной информации до нарушения или предполагаемого нарушения. CPRA §1798.100 (e). Административные штрафы в соответствии с CPRA остаются значительными - 2500 долларов за каждое нарушение и 7500 долларов за каждое умышленное нарушение. CPRA §1798.155.

Компании должны планировать соблюдение требований прямо сейчас, следя за нормативными разъяснениями до даты вступления в силу. Планирование соответствия должно включать анализ рисков цепочки поставок, внутренней системы и персонала для всех категорий личной информации. Организации должны учитывать необходимость договорных гарантий, а также определять меры защиты кибербезопасности, а также процессы оценки рисков и аудита, которые могут потребоваться в свете усовершенствований CPRA к CCPA. Любые вопросы, касающиеся CPRA или CCPA, можно направлять Брайану Г. Чезаратто или другому члену группы EBG по конфиденциальности, кибербезопасности и управлению данными». ***(Brian G. Cesaratto, Deanna Ballesteros. Organizations Should Plan in 2021 to Comply with the California Privacy Rights Act's Enhanced Cybersecurity Safeguards // Epstein Becker & Green, P.C.(https://www.workforcebulletin.com/2021/01/14/organizations-should-plan-in-2021-to-comply-with-the-california-privacy-rights-acts-enhanced-cybersecurity-safeguards/). 14.01.2021).***

***

«В результате неправильной конфигурации облака, совершенной SocialArks, было обнаружено 318 миллионов записей, полученных из Facebook, Instagram и LinkedIn.

Более 400 ГБ данных общедоступных и частных профилей для 214 миллионов пользователей социальных сетей со всего мира были доступны в Интернете, включая информацию о знаменитостях и влиятельных лицах в социальных сетях в США и других странах.

Утечка связана с неправильно настроенной базой данных ElasticSearch, принадлежащей китайской компании SocialArks, занимающейся управлением социальными сетями, которая, по словам исследователей из Safety Detectives, содержала личную информацию (PII) от пользователей Facebook, Instagram, LinkedIn и других платформ.

По словам исследователей, сервер был открыт для публичного доступа без защиты паролем или шифрования во время регулярных проверок IP-адресов потенциально незащищенных баз данных. Всего он содержал более 318 миллионов записей.

Платформа управления данными SocialArks используется для программной рекламы и маркетинга. Она позиционирует себя как «трансграничная компания по управлению социальными сетями, занимающаяся решением текущих проблем построения бренда, маркетинга, маркетинга и управления социальными клиентами во внешней торговле Китая».

Затронутый сервер, размещенный на Tencent, был сегментирован на индексы для хранения данных, полученных из каждого источника в социальных сетях, что позволило исследователям глубже изучить данные.

«Наша исследовательская группа смогла определить, что вся утечка данных была «скопирована» с платформ социальных сетей, что является неэтичным и нарушает условия обслуживания Facebook, Instagram и LinkedIn», - заявили исследователи в блоге в понедельник. сообщение.

Очищенные профили включали 11 651 162 профиля пользователей Instagram; 66 117 839 профилей пользователей LinkedIn; 81 551 567 профилей пользователей Facebook; и 55 300 000 профилей Facebook, которые были удалены в течение нескольких часов после обнаружения открытого сервера.

Данные общедоступного профиля включали биографии, изображения профиля, общее количество подписчиков, настройки местоположения, контактные данные, такие как адреса электронной почты и номера телефонов, количество подписчиков, количество комментариев, часто используемые хэштеги, названия компаний, должность и многое другое.

«Данные социальных сетей, собираемые в маркетинговых целях, неизбежно будут включать конфиденциальную информацию», - сказал Threatpost Джек Маннино, генеральный директор nVisium. «На каждого человека, заботящегося о конфиденциальности и пользующегося социальными сетями, приходится экспоненциально большее количество людей, публично делящихся интимными подробностями своей частной жизни. Чтобы защитить себя, ограничьте публичный доступ к вашему профилю и медиаресурсам, внимательно относитесь к тому, что вы публикуете в Интернете, и будьте осторожны при выборе разрешений, которые вы предоставляете приложениям, которые могут злоупотреблять, использовать или украсть вашу информацию».

Однако, помимо сопоставления общедоступных данных, база данных по необъяснимым причинам также включала личные данные пользователей социальных сетей.

«В базе данных SocialArks хранились личные данные пользователей Instagram и LinkedIn, такие как частные номера телефонов и адреса электронной почты для пользователей, которые не разглашали такую информацию публично в своих учетных записях», - сказали исследователи. «Как SocialArks вообще мог получить доступ к таким данным, остается неизвестным… Остается неясным, как компании удалось получить частные данные из нескольких защищенных источников… Более того, сервер компании имел недостаточную защиту и оставался полностью незащищенным».

Threatpost обратился в SocialArks за дополнительной информацией.

База данных была защищена SocialArks в тот же день, когда службы безопасности сообщили компании о проблеме.

SocialArks пострадал от аналогичной утечки данных в августе, от которой пострадали 66 миллионов пользователей LinkedIn, 11,6 миллиона учетных записей Instagram и 81,5 миллиона учетных записей Facebook - всего около 150 миллионов. Предоставленная информация также состояла из извлеченных общедоступных данных, таких как полные имена, страна проживания, место работы, должность, данные подписчика и контактная информация, а также прямые ссылки на профили.

Эксперты предупреждают, что наличие центрального хранилища такой информации открывает двери для массовых автоматизированных атак социальной инженерии.

«Большая часть сбора данных совершенно безобидна и выполняется веб-разработчиками, аналитиками бизнес-аналитики, честными предприятиями, такими как сайты бронирования путешествий, а также выполняется в целях исследования

рынка в Интернете», - заявили исследователи. «Однако, даже если такие данные получены законным путем - если они хранятся без надлежащей кибербезопасности, могут произойти крупные утечки, затрагивающие миллионы людей. Когда личная информация, включая номера телефонов, адреса электронной почты и информацию о рождении, извлекается и / или утекает, преступники получают право совершать чудовищные действия, включая кражу личных данных и финансовое мошенничество».

Дирк Шрадер, вице-президент New Net Technologies по всему миру, сказал, что тот факт, что сборка вообще проводилась - публичной или частной - представляет интерес.

«Публичные профили очищались и раньше, и гиганты в этой области обычно пытаются блокировать попытки массового очищения, поскольку их намерение состоит в том, чтобы получить доступ к своей «нефти», - сказал он Threatpost. «Интересно было бы узнать, почему в данном случае это не сработало. Как вероятный пользователь LinkedIn, мой выбор ограничен. Либо я согласен с тем, что парсинг будет происходить, либо я могу уменьшить свой профиль, что в определенной степени ограничивает мои возможности устанавливать деловые связи. Сколько информации предоставляет пользователь - это их выбор. Само по себе парсинг, особенно когда собранные данные настолько плохо защищены, увеличивает вероятность стать объектом конкретных атак и нежелательных писем». ***(Tara Seals. Millions of Social Profiles Leaked by Chinese Data-Scrapers // Threatpost (https://threatpost.com/social-profiles-leaked-chinese-data-scrapers/162936/). 11.01.2021).***

***

«Страны Африки и Ближнего Востока принимают законы о конфиденциальности данных головокружительными темпами в течение последних нескольких лет, намного превышая темпы в других регионах мира, таких как Азия и Америка. За последнее десятилетие в этом регионе было принято 24 закона; 14 из них произошли только за последние пять лет. Для сравнения: за тот же 10-летний период было принято 13 новых законов в Азии и 21 в Америке. Все указывает на то, что правила конфиденциальности в регионе будут продолжать расти быстрыми темпами в 2021 году и в последующий период. Правоприменение также, вероятно, усилится в регионе по мере того, как все больше стран создают свои органы по защите данных и эти режимы конфиденциальности начинают созревать.

Этот регион имеет некоторые очень отличительные характеристики, которые отличают его от других регионов мира, особенно в отношении требований к трансграничному переводу и регистрации. Вопреки мировой тенденции минимизировать требования к регистрации, большинство законов в этом регионе требует, чтобы организации регистрировали деятельность по обработке данных в органе защиты данных (DPA). Более того, с его разнообразным набором международных правил ландшафт конфиденциальности данных в этом регионе сродни Дикому Западу.

Взрыв новых и несопоставимых законов в этом регионе за такой относительно короткий период времени в сочетании с тем фактом, что почти треть этих юрисдикций еще не учредили свои DPA, затрудняет для компаний разработку своих региональных подходов к соблюдению конфиденциальности. не говоря уже о том, чтобы интегрировать их в свои глобальные программы соответствия. Тем не менее, важно учитывать эти различия при разработке программ обеспечения конфиденциальности. В этом предупреждении обсуждаются некоторые общие черты и различия между режимами конфиденциальности в регионе и определяются юрисдикции, которые могут принять новые или измененные законы в ближайшие несколько лет.

Характеристики современного регионального ландшафта: общие черты и различия

В 34 юрисдикциях региона действуют всеобъемлющие законы о конфиденциальности. Более двух третей этих законов (24) были приняты в течение последнего десятилетия, и 14 из них были приняты за последние пять лет. Новейшие законы действуют в Республике Конго, Египте, Кении, Нигерии, Того и Уганде. Кроме того, за последние три года были внесены поправки в существующие законы Бенина, Маврикия и ОАЭ (DIFC и ADGM).

Хотя они используют одни и те же основные элементы защиты данных, все эти законы содержат определенные правила, которые сильно отличаются друг от друга и от правил других регионов. Однако реализация программ обеспечения конфиденциальности данных в соответствии с этими правилами может быть сложной задачей, особенно в тех юрисдикциях, которые еще не установили свои DPA.

Объем. Большинство законов в этом регионе применяются только к обработке внутри страны. Однако в трех странах действуют экстерриториальные положения: Бенин, Катар и Уганда. Закон Бенина применяется к обработке, осуществляемой контролерами или обработчиками в Бенине, независимо от того, происходит ли обработка в Бенине или за его пределами. Это также относится к контроллерам и обработчикам, не зарегистрированным в Бенине, которые обрабатывают личную информацию людей в Бенине, если эти действия по обработке относятся к:

- предложение товаров или услуг людям в Бенине вне зависимости от того, обязаны они платить или нет;
- мониторинг поведения отдельных лиц, поскольку это поведение имеет место в Бенине; или же
- обработка, которая происходит в государстве-члене Экономического сообщества западноафриканских государств (ЭКОВАС).

Закон Катара применяется к обработке контролерами, обработчиками и операторами веб-сайтов, а закон Уганды применяется к организациям в Уганде, которые обрабатывают личную информацию, или организациям за пределами Уганды, которые обрабатывают личную информацию, касающуюся граждан Уганды.

Трансграничные переводы. В то время как большинство юрисдикций (31) налагают ограничения на трансграничную передачу персональных данных,

существует такой разнообразный набор правил, что практически невозможно дать им содержательную характеристику.

Достаточность. Двадцать девять из 31 страны разрешают переводы в страны, которые обеспечивают адекватную защиту; однако большинство (24) не опубликовали свои списки адекватных стран. Из пяти списков их списки сильно различаются. Например, Кот-д'Ивуар признает государства-члены ЭКОВАС; Чад признает государства-члены Центральноафриканского экономического и валютного сообщества (CEMAC) и Экономического сообщества центральноафриканских государств (CEEAC); Лесото признает государства-члены, которые изменили требования Сообщества по вопросам развития стран юга Африки (САДК) по защите данных; Марокко признает государства-члены ЕЭЗ и Канаду; ОАЭ / DIFC и ADGM признают государства-члены ЕЭЗ, а также другие юрисдикции, признанные ЕС, как обеспечивающие адекватную защиту.

Для перевода в соответствующую страну восьми из этих 29 стран дополнительно требуется разрешение DPA, уведомление или лицензия DPA: Бенин, Республика Конго, Египет, Гвинея, Марокко, Сенегал, Того и Тунис. Две из этих стран, Республика Конго и Того, еще не создали DPA.

Адекватные меры защиты. Двадцать две из 29 стран разрешают переводы при наличии адекватных мер защиты, таких как договорные положения, но во многих случаях DPA также должны утверждать переводы и / или договорные положения. Лишь несколько DPA (в зонах свободной торговли ОАЭ / DIFC и ADGM) издали свои собственные положения. В качестве альтернативы Израиль разрешает использование стандартных договорных условий ЕС с небольшими изменениями.

Правовые основы. Все законы, кроме нескольких, разрешают переводы в неадекватные страны при условии, что применяется одна из правовых оснований, указанных в законе. Однако эти правовые основы сильно различаются. Некоторые предусматривают одну или несколько юридических оснований, таких как согласие, договорная необходимость, жизненные интересы и / или юридическое требование; некоторые разрешают такие передачи только на основании согласия, в то время как другие ограничивают использование согласия передачами, которые являются ограниченными и конкретными. Многие законы также требуют разрешения DPA для таких переводов. Напротив, законы таких стран, как Буркина-Фасо, Кот-д'Ивуар, Гвинея, Нигер и Тунис, не предоставляют никаких юридических оснований, кроме разрешения DPA.

Уведомление о нарушении. Более одной трети законов (14) требуют уведомления в случае утечки данных. В пяти юрисдикциях не требуется уведомления физических лиц и / или DPA, если нет риска причинения вреда от нарушения. Остальные девять юрисдикций требуют уведомления DPA в случае нарушения безопасности данных. Хотя многие законы требуют, чтобы уведомление было направлено физическим лицам и / или DPA «в кратчайшие возможные сроки» или «без промедления», другие (Республика Конго, Египет, Маврикий и ОАЭ / ADGM) требуют уведомления. в DPA в течение 72 часов. Большинство требует, чтобы о нарушении были уведомлены как отдельные лица, так и DPA.

Правовые основы обработки. Почти половина законов (16) не разрешает обработку на основании законных интересов. Вместо этого законы полагаются на другие правовые основы, такие как согласие, договорная необходимость, юридические требования или жизненные интересы. Только две страны, Израиль и Мали, прямо не требуют юридической основы для обработки. Вместо этого они указывают, что обработка для целей, отличных от тех, для которых была предоставлена информация, является нарушением конфиденциальности.

Индивидуальные права. Права доступа и исправления должны быть предоставлены во всех странах. Более двух третей законов (24) предоставляют права на стирание, а одна четверть (8) - права на переносимость данных. Сроки ответа на индивидуальные запросы о правах также сильно различаются: 12 стран требуют ответа на запросы о правах в течение 30 дней или более; два в течение 21 дня; восемь в течение 10-15 дней; и один в течение шести дней. Десять не указывают конкретный период времени.

Сотрудник по защите данных (DPO). Более четверти юрисдикций (10) требуют назначения DPO: Бенин, Республика Конго, Египет, Мадагаскар, Маврикий, Нигерия, Южная Африка, Тунис, Уганда и ОАЭ / DIFC.

Регистрация. В то время как во всем мире наблюдается тенденция к минимизации требований к регистрации, большинство законов в регионе (31) требуют, чтобы организации регистрировали деятельность по обработке данных в DPA. Страны, которые не предъявляют требований к регистрации, - это Республика Конго, Нигерия и Катар.

Безопасность. Чуть более половины стран (18) имеют конкретные или очень подробные положения о безопасности. Страны с подробными обязательствами по обеспечению безопасности - это Бенин, Израиль, Сенегал и ОАЭ / DIFC. Три страны, Бенин, Кот-д'Ивуар и Нигерия, требуют ежегодного представления DPA отчетов о соблюдении требований безопасности или аудита.

Оценка воздействия на защиту данных (DPIA). Большинство законов в регионе не требует от организаций проведения DPIA. DPIA требуются только в Бенине, Республике Конго, Израиле, Кении, Маврикии, Южной Африке и ОАЭ / DIFC.

Исполнение. С вступлением в силу нескольких новых законов за последние два года и недавним созданием DPA в Кении и Уганде, которые, скорее всего, последуют в следующем году или около того, правоприменительная деятельность в регионе, вероятно, возрастет. DPA в Бенине, Гане, Израиле, Мали, Маврикии, Марокко, Сенегале и Тунисе были наиболее активными; DPA в Нигерии и Южной Африке также, вероятно, скоро присоединятся к этому списку. В прошлом году нигерийское DPA начало выдавать уведомления о несоответствии организациям, которые не представили требуемые аудиты защиты данных. В Южной Африке DPA была создана на пару лет, но вступление в силу закона о конфиденциальности данных начнется не раньше 1 июля 2021 года.

Недавно принятые законы о конфиденциальности

Ниже приводится краткая информация о недавно принятых законах:

Бахрейн. Закон Бахрейна о защите личных данных, Закон № 30 от 2018 года, вступил в силу 1 августа 2019 года. DPA еще не создан; однако Министерство

юстиции временно приняло на себя свои функции и полномочия до тех пор, пока независимому органу не будет выделен бюджет и не будет создан совет директоров.

Республика Конго. Закон № 29-2019 о защите персональных данных вступил в силу в ноябре 2019 года; соблюдение требований организациями частного сектора требовалось к ноябрю 2020 года. DPA еще не установлен.

Египет. Закон о защите персональных данных № 151 от 2020 года вступил в силу 14 октября 2020 года; соблюдение требований требуется через год после издания исполнительных правил. Ожидается, что эти правила будут выпущены к 14 апреля 2021 года. DPA еще не создана.

Кения. Закон о защите данных 2019 года вступил в силу в ноябре 2019 года; однако уполномоченный по защите данных был назначен совсем недавно, в ноябре 2020 года.

Нигерия. Положение о защите данных 2019 г. («Положение») было издано Национальным агентством по развитию информационных технологий (NITDA) в январе 2019 г. Впоследствии NITDA выпустило проект Основы реализации защиты данных для Регламента, который он призвал компании использовать в качестве руководства по соблюдению требований до выпускается окончательный текст. Окончательный текст еще не опубликован в окончательной форме. Между тем, как обсуждается ниже, сейчас предпринимаются усилия по разработке нового, более всеобъемлющего закона о защите данных.

Южная Африка. Несмотря на то, что он был принят в 2013 году, Закон Южной Африки о защите личной информации вступил в силу только 1 июля 2020 года. Организациям было предоставлено право до 1 июля 2021 года, чтобы соблюдать закон. DPA действует с 2016 года.

Идти. Закон о защите персональных данных вступил в силу в октябре 2019 года, а его исполнение началось в октябре 2020 года; однако DPA еще не создана.

Уганда. Закон Уганды о защите данных и конфиденциальности 2019 года был принят в феврале 2019 года и вступил в силу в феврале 2020 года. Тем не менее, необходимые подзаконные акты еще не изданы. Министерство ИКТ и Национальное руководство опубликовали для общественного обсуждения Проект Правил защиты данных и конфиденциальности 2020 («Проект Правил»), в котором, среди прочего, рассматриваются положения, касающиеся регистрации, уведомления о нарушении безопасности и требований DPO. Закон предусматривает создание отдела защиты данных в Национальном управлении информационных технологий; однако в настоящее время нет никаких указаний на открытие этого офиса.

ОАЭ / DIFC. Новый закон о защите данных, Закон DIFC № 5 от 2020 года, вступил в силу 1 июля 2020 года, заменив Закон о защите данных DIFC 2007 года. В ответ на пандемию правительство объявило, что предприятиям, подпадающим под действие закона, будет предоставлен трехмесячный льготный период до 1 октября 2020 года для приведения в соответствие с законом. Хотя закон в целом соответствует Общему регламенту ЕС по защите данных, есть некоторые заметные различия в положениях, касающихся, например, согласия, индивидуальных прав, регистрации и уведомления о нарушении безопасности.

Новые законы ожидаются в 2021 году и в последующий период

Ожидаемые поправки к существующим законам

Израиль. Спустя почти 40 лет после вступления в силу Закона Израиля о защите конфиденциальности 5741-1981 годов министерство юстиции Израиля объявило в 2020 году о своих планах обновить закон с учетом новых технологических достижений. В декабре 2020 года он провел консультации, чтобы запросить мнение общественности о способах внесения поправок в закон. Кроме того, с 2018 года предпринимаются усилия по улучшению и обновлению надзорных и правоприменительных возможностей DPA.

События в странах, где нет законов о конфиденциальности

В ближайшие пару лет мы ожидаем принятия новых законов, возможно, в Иордании, Намибии, Нигерии, Саудовской Аравии и Зимбабве:

Иордания. Министерство цифровой экономики и предпринимательства представило свой проект закона о защите данных в Совет министров, и в январе 2020 года законопроект был опубликован на сайте Бюро законодательства и мнений. В случае принятия законопроект, среди прочего, установит общие принципы защиты данных, потребует юридических оснований для обработки личных данных, обеспечит индивидуальные права, включая право на забвение и переносимость данных, установит требования к 72-часовому уведомлению о нарушениях и ограничит трансграничная передача персональных данных в страны, которые обеспечивают адекватные правила защиты. DPA будет учреждено в рамках Министерства цифровой экономики и предпринимательства.

Намибия. Сообщается, что Министерство информационных и коммуникационных технологий (MICT) работает над проектом закона о защите данных. В феврале 2020 года Министерство участвовало в семинаре по разработке законодательства о защите данных, спонсором которого был Совет Европы.

Нигерия. Правительство Нигерии разработало закон о защите данных, закон о защите данных, 2020 г., который, как ожидается, будет внесен в Национальное собрание. В отличие от практически всех других законов, принятых во всем мире, предлагаемый закон будет регулировать личные данные физических и юридических лиц (как государственных, так и частных). Кроме того, он будет применяться к обработке контроллерами, созданными в Нигерии, контроллерами, не зарегистрированными в Нигерии, которые используют оборудование в Нигерии для обработки персональных данных, а также контроллерами (без учета их учреждения), которые выполняют обработку информации, касающейся лиц, которые проживают в пределах или за пределами Нигерии, а также личные данные, которые частично или полностью происходят из Нигерии. Как и другие законы, это законодательство устанавливает основные принципы и правовые основы (такие как законные интересы, договорная необходимость и согласие) для обработки персональных данных, обеспечивает права личности, включая права на стирание и перенос данных, и налагает требования безопасности, включая особые обязательства на обработчиков данных. Кроме того, он налагает ограничения на трансграничные переводы и требует представления ежегодных аудиторских отчетов и уведомления об утечках данных в течение 48 часов. Наконец, он

предусматривает создание Комиссии по защите данных и предусматривает уголовное наказание за нарушение закона.

Саудовская Аравия. Национальное управление данных Саудовской Аравии (NDMO), организация, отвечающая за управление данными в Королевстве, недавно издало Временные правила национального управления данными. («Временные правила»), но их правовой статус (являются ли они обязательными нормативными актами или добровольными указаниями) остается неясным. Временные правила касаются таких областей, как классификация данных, совместное использование данных и конфиденциальность данных, в ожидании дальнейших правил или законодательства в этой области. Положения, касающиеся конфиденциальности данных, среди прочего, налагают требования к локализации данных, которые требуют от контроллеров хранить и обрабатывать персональные данные в пределах страны, если только контроллеры не получат письменное предварительное разрешение от регулирующих органов, и требуют согласия на обработку персональных данных в большинстве случаев и уведомления об утечке данных в течение 72 часов.

Зимбабве. Cyber Security и Билл Защита данных в настоящее время находитсярассмотрении в парламенте. В прошлом году прошли общественные слушания и консультации по предложенному закону, и ожидается, что законодательный орган примет законопроект в 2021 году. Законопроект вызвал споры, в основном в отношении положений, которые криминализируют определенные формы онлайн-выступления и деятельности. Критики утверждают, что эти положения подорвут свободу слова и свободу СМИ. Что касается положений, касающихся защиты данных, законопроект устанавливает общие правила обработки персональных данных, включая конфиденциальные данные, такие как генетические, биометрические данные и данные о состоянии здоровья, а также вводит требования об уведомлении, согласии и уведомлении о нарушениях…» ***(Cynthia J. Rich. Out of Africa (and the Near East): Privacy Rules Come at Rapid Pace // Morrison & Foerster (https://www.mofo.com/resources/insights/210111-africa-near-east-privacy-rules.html). 11.01.2021).***

***

«Правительство Великобритании оценивает возможные последствия «технической ошибки», из-за которой из полицейских баз данных были удалены 150 тыс. записей, в том числе отпечатков пальцев подозреваемых, образцов ДНК и информация об арестах.

Как сообщает The Times, в результате инцидента преступники могли остаться безнаказанными, поскольку собранные с мест преступлений биометрические вещественные доказательства не отмечались в электронной системе Police National Computer (PNC), где хранятся данные по уголовным расследованиям. Правоохранительные органы используют PNC для получения сведений, способных помочь в расследованиях общенациональных, региональных и местных уголовных дел.

Ошибка программного обеспечения не только стала причиной исчезновения из Police National Computer критически важной информации о подозреваемых, но также привела в беспорядок британскую визовую систему. Выдача британских виз была приостановлена на два дня, поскольку полицейская база данных используется для проверки заявителей на наличие совершенных правонарушений.

По данным источников The Times, 150 тыс. записей об арестованных были случайно удалены во время очередной еженедельной «очистки» от данных, срок хранения которых уже истек (британские власти обязаны удалять данные о задержанных, которые не были осуждены, после трех лет хранения). Возможность злонамеренной активности, например, кибератаки, была исключена.

Как сообщает Министерство внутренних дел Великобритании, удаленные записи касаются лиц, которые были арестованы, но затем отпущены без каких-либо дальнейших действий. Тем не менее, по мнению представителей Лейбористской партии Великобритании, инцидент представляет огромную угрозу общественной безопасности, пишет BBC. Потеря данных в результате технической ошибки может помешать дальнейшим полицейским расследованиям, потому что отпечатки пальцев и образцы ДНК подозреваемых нельзя будет сопоставить с доказательствами с других мест преступления.

Министр полиции, охраны и общественной безопасности Великобритании Кит Малтхаус (Kit Malthouse) уверил, что причина проблемы уже выявлена, а в процедуру удаления устаревших записей были внесены корректировки во избежание подобных инцидентов в будущем. В настоящее время Министерство внутренних дел, Совет директора Национальной полиции и другие правоохранительные органы работают «в темпе» над восстановлением утраченных данных». ***(Сбой привел к удалению 150 тыс. данных подозреваемых из БД британской полиции // SecurityLab.ru (https://www.securitylab.ru/news/515550.php).15.01.2021).***

***

«В настоящее время статья 41 Закона КНР о кибербезопасности предусматривает, что личная информация должна собираться только в случае необходимости. В отсутствие судебных указаний одна из проблем, с которыми сталкиваются как операторы приложений, так и частные лица, заключается в том, какая часть личной информации может быть собрана на законных основаниях без нарушения этого требования закона и не будет рассматриваться надзорными регулирующими органами как проводящая чрезмерный сбор. Например, может ли оператор приложения настоять на получении доступа к списку контактов человека, прежде чем он сможет загрузить приложение?

Киберадминистрация Китая (CAC) также заметила, что люди очень часто не имеют выбора, кроме как предоставить личную информацию, если они хотят загрузить приложения.

Ранее в 2020 году правительство КНР начало процесс публикации национального стандарта, устанавливающего ограничения на типы личной информации, которую может собирать оператор приложения. Проект национального стандарта «Технология информационной безопасности - Базовые

спецификации для сбора личной информации в мобильных интернет-приложениях» был должным образом опубликован, и в настоящее время готовится окончательная версия.

Однако, чтобы решить эту проблему чрезмерного сбора, 1 декабря 2020 года CAC опубликовал для консультаций набор проектов правил, озаглавленный «S cope of Needed Personal Information for Common Types of Mobile Internet Applications». Период консультаций был коротким: он закончился 16 декабря 2020 года. Поэтому ожидается, что окончательные правила будут опубликованы в ближайшее время.

Набор правил, предложенный CAC, прост:

в нем перечислены 38 типов приложений (см. список ниже), типы личной информации, которая считается необходимой для правильного базового функционирования приложений, и основные функции этих 38 типов приложений; и

если физическое лицо согласилось предоставить перечисленную информацию, то ему не может быть отказано в установке приложений оператором приложения.

CAC придерживается мнения, что в отношении многих типов приложений физическому лицу не требуется предоставлять личную информацию, прежде чем он сможет установить приложения и пользоваться основными функциями. Примеры включают:

Магазины приложений

Электронные книги

Спорт и фитнес

Браузер

Как уже упоминалось, CAC также определяет основные функции этих 38 типов приложений. Например, для приложения для навигации по карте основная функция - это ориентация / позиционирование и навигация, и поэтому информация, которую должен предоставить человек, - это данные о его местоположении. Другой пример: для приложения по найму основными функциями являются поиск информации о вакансии и отправка резюме, поэтому от человека следует требовать только указать номер своего мобильного телефона (или другую информацию, которая может идентифицировать человека, и оператор приложения должен предоставить варианты для человека на выбор) и его резюме.

Наблюдения

Что может представлять собой чрезмерный сбор, вероятно, станет актуальной проблемой в будущем, особенно когда принцип защиты данных минимизации данных теперь официально включен в проект Закона КНР о личной информации (см. Ст. 6) (Примечание: этот принцип уже существует в Национальный стандарт «Технологии информационной безопасности - Спецификация безопасности личной информации», который действует с 2017 года). Если правила опубликованы в их нынешних формах, они действительно содержат очень практические рекомендации как для операторов приложений, так и для отдельных лиц, поскольку требования и ограничения носят довольно предписывающий характер.

Стоит отметить, что там, где приложение предоставляет больше, чем базовые функции, перечисленные CAC, операторы приложений теоретически должны

иметь право определять дополнительную личную информацию, требуемую от лиц, в пределах параметров, установленных применимыми правилами защиты данных. Может ли такой сбор стать результатом чрезмерного сбора, будет зависеть от судебной разработки концепции минимизации данных в Китае…» ***(Michelle Chan, Clarice Yue. A curb on what personal information is necessary for your app – proposed rule by the Cyber Administration of China // Bird & Bird (https://www.twobirds.com/en/news/articles/2021/china/a-curb-on-what-personal-information-is-necessary-for-your-app). 12.01.2021).***

***

«Этот электронный бюллетень обобщает последние разработки в области кибербезопасности и защиты данных в Китае. Мы фокусируемся на четырех областях: нормативно-правовая база, правоприменение, промышленность и международные разработки.

Наши основные моменты

Постоянный комитет Всекитайского собрания народных представителей продолжит рассмотрение Закона о безопасности данных и Закона о защите личной информации в 2021 году, как и планировалось. Его цель - как можно скорее обнародовать законы. Мы будем держать вас в курсе последних событий.

Гражданский кодекс вступил в силу 1 января 2021, а также обеспечивает защиту гражданского права личной информации. В последнем судебном толковании Гражданского кодекса Верховный народный суд прямо включил «спор о защите личной информации» в качестве уважительной причины для возбуждения гражданского иска. В результате мы ожидаем увеличения количества гражданских дел, возбужденных в соответствии с Гражданским кодексом за нарушение личных данных.

Нормативные разработки

1. Верховный народный суд добавляет «спор о защите личной информации» в качестве нового основания для иска.

30 декабря 2020 года Верховный народный суд опубликовал свое судебное толкование Гражданского кодекса, в котором были пересмотрены основания для возбуждения исков по гражданским делам. Что касается защиты данных, в качестве новой причины иска был добавлен «спор о защите личной информации». Гражданский кодекс теперь предоставляет правовую основу для обращения за средствами правовой защиты в случае незаконного обращения с личной информацией, а также несет ответственность за незаконную обработку личной информации. Кроме того, судебное толкование также добавило другие причины для иска, такие как защита голоса и возможность ходатайствовать о судебном запрете, чтобы остановить нарушение прав личности. Уточнено определение телесных повреждений и размер компенсации.

2. Обзор Закона о безопасности данных и Закона о защите личной информации продолжится в 2021 году.

21 декабря 2020 года Постоянный комитет Всекитайского собрания народных представителей подтвердил, что продолжит пересмотр Закона о безопасности данных и Закона о защите личной информации (PIPL) в 2021 году в соответствии

со своим планом работы в области законодательства. Проект PIPLсодержит специальные положения о распознавании лиц, требующие, чтобы личная биометрическая информация могла использоваться только для определенных целей и при условии, что ее использование необходимо (на основе предварительной оценки). Такую информацию также следует использовать только в минимально необходимом объеме. Применение и развитие распознавания лиц поставили много новых задач в области защиты личной информации. Комиссия по законодательным вопросам продолжит консультации и выяснение мнений по соответствующим вопросам.

3. Новые рекомендации по созданию стандартных систем безопасности данных в телекоммуникационной и интернет-индустрии.

25 декабря 2020 года Министерство промышленности и информационных технологий выпустило новые инструкции по созданию стандартных систем безопасности данных в телекоммуникационной и интернет-индустрии. В них изложены детали структуры безопасности данных и уровней классификации данных. Ключевые технические стандарты регулируют основные технологии безопасности данных, охватывающие такие аспекты, как сбор, передача, хранение, обработка, обмен и уничтожение данных. Стандарты управления безопасностью, предусмотренные в руководствах, включают правила безопасности данных, оценку безопасности данных, мониторинг, раннее предупреждение и обработку рисков.

4. Проект руководящих принципов в отношении объема необходимой личной информации для распространенных типов мобильных интернет-приложений.

1 декабря 2020 года Администрация киберпространства выпустила для общественного обсуждения проект руководящих принципов в отношении объема личной информации, которую необходимо собирать для обычных типов мобильных приложений для нормальной работы. Руководящие принципы направлены на регулирование сбора личной информации приложениями и обеспечение безопасности личной информации граждан. Проект руководящих принципов ограничивает объем необходимой личной информации, которую необходимо собирать 38 типами приложений, включая приложения для навигации по карте, онлайн-вызова автомобиля, обмена мгновенными сообщениями, онлайн-платежей, онлайн-покупок, доставки еды, логистики, транспортировки и продажи билетов, работы охота, онлайн-кредиты, короткие видеоролики, аренда и продажа жилья.

5. Приняты новые меры по усилению сетевой безопасности и защиты информации для страховых компаний в Интернете.

14 декабря 2020 года Комиссия по регулированию банковской и страховой деятельности Китая издала новые нормативные меры по надзору за страховым бизнесом в Интернете, которые вступят в силу 1 февраля 2021 года. Эти меры усиливают требования к сетевой безопасности и защите информации клиентов и устанавливают надзорную информацию. система для усиления информационной отчетности и улучшения надзора. Эти меры, основанные на стандартных операциях и предотвращении рисков, способствуют интеграции страхования с новыми технологиями, такими как Интернет, большие данные и цепочка блоков. Эти меры также способствуют расширению источников информации о данных и

использованию интеллектуального анализа данных, машинного обучения и других технологий для повышения точности выявления рисков и обработки страхового бизнеса.

6. Судебное толкование гражданских споров, связанных с безопасностью пищевых продуктов, устанавливает ответственность платформ электронной торговли.

9 декабря 2020 года Верховный суд издал судебное толкование гражданских споров, связанных с безопасностью пищевых продуктов, которое вступило в силу 1 января 2021 года. В нем четко изложены обязательства в отношении платформ электронной торговли и обстоятельства, при которых они будут обязаны выплатить компенсацию. Например, если платформа электронной коммерции не может выполнить регистрацию настоящего имени или проверить лицензии операторов питания, или не может сообщить или прекратить предоставление услуг в соответствии с законом, в результате чего потребителям причинен ущерб, платформа электронной коммерции и операторы питания несут солидарную ответственность.

7. Новые правила онлайн-услуг по найму

24 декабря 2020 года Министерство кадров и социального обеспечения издало новые правила администрирования онлайн-услуг по найму, которые вступят в силу 1 марта 2021 года. Эти правила охватывают требования к доступу, кодекс поведения, надзор, управление и юридические вопросы. обязанности по найму онлайн. Они запрещают незаконное раскрытие, продажу и предоставление личной информации третьим лицам. Правила также побуждают кадровые агентства использовать большие данные, цепочку блоков и другие технические меры для обеспечения безопасности онлайн-сервисов найма и предотвращения незаконной онлайн-деятельности.

8. Положение о продвижении цифровой экономики в провинции Чжэцзян.

24 декабря 2020 года были изданы новые правила продвижения цифровой экономики в провинции Чжэцзян, которые вступят в силу 1 марта 2021 года. Эти правила в основном охватывают цифровую инфраструктуру, ресурсы данных, цифровую индустриализацию, цифровизацию промышленности, цифровое управление, стимулы. защитные меры и юридическая ответственность.

9. Запланированы временные положения о защите личной информации приложениями.

24 декабря 2020 года Министерство промышленности и информационных технологий объявило, что проведет исследование и сформулирует временные положения о защите личной информации с помощью приложений. Основное внимание в исследовании уделяется продвижению специальных мер по исправлению ситуации, когда приложения нарушают права и интересы пользователей, выпуску серии стандартов для защиты личной информации приложениями, созыву национального собрания по надзору и администрированию для рассмотрения проблемы и созданию национальной платформы тестирования Программы.

Развитие правоприменения

1. Выпущена шестая партия приложений, нарушающих права пользователей.

3 декабря 2020 года Министерство промышленности и информационных технологий опубликовало шестое в своей серии уведомлений, содержащих подробную информацию о приложениях, которые нарушили права и интересы пользователей. Он отметил, что 60 приложений не приняли необходимых мер по исправлению положения, причем крайний срок для этого - 10 декабря 2020 года. Приложения по умолчанию включают четыре приложения для онлайн-образования, восемь онлайн-приложений для путешествий, два приложения для брака и свиданий, медицинское приложение и два интернет-приложения для спорта и фитнеса.

2. Выпущена седьмая партия приложений, нарушающих права пользователей.

21 декабря 2020 года Министерство промышленности и информационных технологий выпустило седьмую серию уведомлений, содержащих подробную информацию о приложениях, нарушающих права и интересы пользователей. Он отметил, что 63 приложения не смогли внести необходимые исправления, и они должны сделать это до 28 декабря 2020 года. Среди отмеченных проблем были проблемы с частным сбором информации о MAC-адресах устройства и отправкой личной информации пользователей в сторонние SDK без согласия пользователей. Некоторые магазины приложений и платформы распространения мобильных приложений намеренно избегали наблюдения с помощью технических средств. Следующие шаги против этих приложений и соответствующих компаний включают полное удаление, приостановку доступа и административные санкции.

3. Первое дело о нарушении неприкосновенности частной жизни граждан в связи с Covid-19.

18 декабря 2020 года стало известно, что суд Юбэй рассмотрел первое дело о нарушении прав на неприкосновенность частной жизни в связи с Covid-19. В судебном решении ответчику, компании Chongqing Marketing Planning Co., Ltd., было предписано опубликовать письменные извинения на своем официальном сайте и в газете, а также выплатить истцу компенсацию в размере 1 юаня за моральный ущерб. замороженные креветки, импортированные из Эквадора, которые дали положительный результат на Covid-19. Ответчик опубликовал на своем официальном сайте данные о более чем 10 000 клиентов (включая подробные сведения об их именах, домашних адресах, идентификационных номерах и другую подробную личную информацию), которые приобрели креветки. Суд постановил, что, хотя дело относилось к чрезвычайному периоду, требования истца имели основания.

4. Первый иск, связанный с нарушением прав на неприкосновенность частной жизни в Интернете.

3 декабря 2020 года Народной прокуратурой Баодина был заслушан иск, связанный с общественными интересами, против 65 человек, которые использовали Интернет для нарушения прав других лиц на конфиденциальность. Обвиняемые использовали программу для написания программного обеспечения для расшифровки, которое взламывало оборудование для наблюдения за подглядыванием и продавало программное обеспечение другим лицам. Суд установил, что это нарушило частную жизнь других лиц и нанесло ущерб общественному благосостоянию. Суд потребовал от ответчиков удалить и

прекратить продажу программного обеспечения, устранить причиненный ущерб и принести публичные извинения национальным СМИ. Этот случай является первым судебным процессом, представляющим общественный интерес, в связи с нарушением конфиденциальности посредством неправомерного использования Интернета.

5. В 17 туристических приложениях обнаружены проблемы с конфиденциальностью

17 декабря Национальный центр экстренного реагирования на компьютерные вирусы обнаружил, что 17 туристических приложений имеют проблемы с конфиденциальностью, поскольку собирают личную информацию за пределами разрешенного объема. Нарушения делятся на пять основных категорий: (i) неспособность убедить пользователей прочитать политику конфиденциальности очевидным образом; (ii) не предоставлять пользователю все разрешения на конфиденциальность; (iii) не перечислять по отдельности каждую из целей, методов, объема сбора и использования личной информации; (iv) установление необоснованных условий для аннулирования учетных записей пользователей; и (v) неспособность установить каналы подачи жалоб и сообщений о нарушениях безопасности личной информации или не обрабатывать сообщения / жалобы в разумные сроки.

Развитие отрасли

1. Пятилетний план построения общества, управляемого законами, предлагает управление киберпространством на основе закона.

7 декабря 2020 года Центральный комитет Коммунистической партии Китая опубликовал пятилетний план (2020-2025 годы) по построению общества, управляемого законами. План предлагает основанное на законе управление киберпространством и направлено на совершенствование правовой системы в этой области. Основное содержание включает (i) пересмотр правил, касающихся информационных услуг в Интернете; (ii) исследование и формулирование правил, касающихся кредитной информации лиц, совершивших серьезную нечестность при предоставлении информационных услуг в Интернете; и (iii) формулирование и совершенствование стандартизированных правил для новых средств массовой информации и новых технологий, таких как онлайн-трансляция в прямом эфире, собственные СМИ, сайты вопросов и ответов и рекомендации по алгоритмам. План предлагает создание и улучшение определенных систем управления кибербезопасностью, например, защита критически важной информационной инфраструктуры, управление безопасностью данных и проверка сетевой безопасности. В нем также предлагается усилить руководство по исследованиям, разработкам и применению новых технологий, таких как большие данные, облачные вычисления и искусственный интеллект, стандартизированным образом. В плане говорится, что Китай будет активно участвовать в разработке международных правил и стандартов в области цифровой экономики, электронной коммерции, информационных технологий и кибербезопасности.

2. Предложены пилотные проекты по управлению безопасностью трансграничных потоков данных.

18 декабря 2020 года Администрация киберпространства Пекина учредила пилотные проекты по управлению безопасностью трансграничных потоков данных. Пилотные проекты в основном расположены в парке программного обеспечения Чжунгуаньцунь, зоне обслуживания международного сотрудничества Цзиньчжань и зоне свободной торговли на территории аэропорта. Они сосредоточены на искусственном интеллекте, биомедицине и других областях и стремятся решить проблемы с международными потоками данных. Пилотные проекты охватывают оценку безопасности трансграничной передачи личной информации и сертификацию возможностей предприятий по защите данных.

Международные разработки

1. Европейская комиссия публикует предложение по Закону о цифровых услугах

15 декабря 2020 года Европейская комиссия опубликовала свое предложение по новому Закону о цифровых услугах, который будет регулировать цифровые услуги, которые соединяют потребителей с товарами, услугами и контентом в качестве посредников. Предлагаемый закон вводит обязательства в отношении цифровых услуг в Европейском союзе, включая правила по удалению незаконных товаров или онлайн-контента. Он установит обязательства для крупных онлайн-платформ по предотвращению злоупотреблений, основанных на риске, и предоставит исследователям более широкие разрешения для облегчения доступа к ключевым данным платформы.

2. Европейская комиссия представляет предложение по Закону о цифровом рынке.

15 декабря 2020 года Европейская комиссия объявила о деталях предлагаемого нового закона о цифровом рынке, который направлен на запрещение недобросовестного поведения «привратников» на онлайн-платформах. Закон направлен на предотвращение того, чтобы такие привратники навязывали несправедливые условия предприятиям и потребителям, а также на обеспечение открытости важных цифровых услуг. Такие критерии, как масштаб влияния внутреннего рынка ЕС и то, контролирует ли организация каналы от коммерческих пользователей до конечных потребителей, будут учитываться при определении того, рассматривается ли организация как привратник. В таком случае на него будут возложены дополнительные обязанности.

3. Twitter оштрафован на 547 000 долларов за нарушение Общего регламента ЕС по защите данных.

15 декабря 2020 года Ирландская комиссия по защите данных сообщила, что наложила штраф в размере 450 000 евро за утечку данных Twitter. В январе 2019 года Twitter не смог своевременно (то есть в течение 72 часов) уведомить регулирующий орган об обнаружении нарушения. Это первое трансграничное дело о наложении штрафов на технологическую компанию США с момента вступления в силу Общего регламента ЕС по защите данных». ***(Mark Robinson, Nanda Lau, James Gong. China Cybersecurity and Data Protection: Monthly Update – Jan 2021 Issue // Herbert Smith Freehills LLP (https://sites-herbertsmithfreehills.vuturevx.com/95/24438/compose-email/china-cybersecurity-and-data-protection--monthly-update---jan-2021-issue.asp). 25.01.2021).***

***

«Сингапур неоднократно подчеркивал необходимость доверия, чтобы внедрение новых технологий могло процветать, но его положение о расширении бизнес-доступа к пользовательским данным - на фоне продолжающихся нарушений безопасности и ошибок - создает тревожные риски впереди. Настоятельно необходимо обеспечить более строгий контроль пользователей над своими личными данными, особенно с учетом того, что правительству самому нужно будет восстановить доверие общества после серьезной ошибки, связанной с попытками страны по отслеживанию контактов COVID-19.

В последние годы Сингапур открывает доступ к данным о гражданах в рамках усилий по облегчению деловых операций и упрощению рабочего процесса. Только в ноябре прошлого года был обновлен Закон о защите личных данных (PDPA), который позволяет местным организациям использовать данные потребителей без предварительного согласия для некоторых целей, таких как улучшение бизнеса и исследования.

Среди ключевых изменений - требование «исключения из согласия», которое позволяет компаниям использовать, собирать и раскрывать данные в «законных целях», для улучшения бизнеса и для более широкого круга исследований и разработок. В дополнение к существующим исключениям согласия, которые включают в себя цели расследований и реагирования на чрезвычайные ситуации, теперь они включают усилия по борьбе с мошенничеством, совершенствованию продуктов и услуг и проведению маркетинговых исследований для понимания потенциальных сегментов клиентов.

Компании также могут использовать данные без согласия для содействия исследованиям и разработкам (НИОКР), которые еще не могут быть отмечены для выпуска продукции.

Были высказаны опасения, что поправки, особенно в отношении исключений и предполагаемого согласия, являются слишком широкими и могут быть использованы организациями для злоупотреблений. «Законные интересы», например, можно рассматривать с точки зрения организации, а ее оценка является субъективной при рассмотрении того, перевешивают ли эти интересы потенциальные неблагоприятные последствия для отдельного лица, что является требованием, изложенным в поправке.

И хотя люди по-прежнему могут отозвать согласие после периода отказа, как они могут это сделать, если они даже не знают, что с самого начала согласились? В соответствии с правилом «исключения из согласия», обязаны ли компании информировать потребителей, что их данные будут использоваться, и как они будут использоваться?

Министр связи и информации Сингапура С. Ишваран объяснил, что данные являются ключевым экономическим активом в цифровой экономике, поскольку они дают ценную информацию, которая информирует предприятия и способствует повышению эффективности. Он также способствует инновациям и совершенствует

продукты и будет важным ресурсом для новых технологий, таких как искусственный интеллект.

Я полностью понимаю, что, в конце концов, доступ к данным - это то, что поддерживает API (интерфейсы прикладного программирования) и подпитывает рыночную конкуренцию.

Однако потребителям необходимо дать возможность решать, кому и как они хотят получать доступ к своим собственным данным, потому что коммерческие предприятия, получив бесплатный буфет, неизбежно будут стремиться получить как можно больше.

Мой банк, например, планирует постепенно отказаться от использования своего физического токена в качестве варианта двухфакторной аутентификации и полностью перейти на цифровые токены. Это означает, что такие клиенты, как я, будут вынуждены загрузить мобильное приложение банка, с которым интегрирован цифровой токен, только для того, чтобы подтвердить мою личность и получить доступ к любым его услугам онлайн-банкинга.

Ключевым разочарованием здесь является то, что приложение банка требует целого ряда разрешений, включая возможность читать мои контактные данные, а также доступ к настройкам Bluetooth моего телефона и данным о местоположении.

Любой внешний доступ к моим личным данным должен быть ограничен только по необходимости. Я считаю, что эта практика имеет важное значение для снижения рисков моей безопасности, особенно с учетом того, что киберугрозы становятся все более изощренными, а утечки данных кажутся неизбежными.

Если крупные компании, такие как RedMart и Grab от Lazada, могут не обращать внимания на лазейки в системе безопасности, которые привели к взломам и компрометации данных клиентов, что еще представляют собой малые предприятия с гораздо более ограниченными ресурсами, которые не могут подключиться, даже если они собирают больше личной информации потребителей?

И что происходит, когда компании решают изменить свои политики использования данных и конфиденциальности? Это может часто происходить, когда происходит поглощение, такое как Facebook и WhatsApp, и мы знаем, что эти компании не всегда выполняют свое обещание поддерживать статус-кво после слияния в отношении данных клиентов. Конечно, пользователи, возмущенные изменением политики конфиденциальности WhatsApp, могут перейти на альтернативы, такие как Signal и Telegram, но что произойдет, когда альтернативы будут выкуплены другим рыночным гигантом, таким как Google, Apple или Microsoft?

Непродуманные бизнес-решения и недостатки в системе безопасности могут подорвать доверие, и когда потребители больше не верят, что их личные данные будут защищены и использоваться ответственно, они откажутся от внедрения новых цифровых услуг и технологий. И это может иметь как неблагоприятные экономические, так и социальные последствия.

УРОКИ ПРОВАЛА В ОТНОШЕНИИ КОНФИДЕНЦИАЛЬНОСТИ TRACETOGETHER

Сингапур должен знать об этом лучше всех, поскольку общественное доверие сильно пострадало, когда выяснилось, что данные отслеживания контактов в

стране с COVID-19 могут быть доступны для различных целей, кроме их первоначального намерения.

Правительство в начале этого месяца признало, что правоохранительные органы могли бы использовать в TraceTogether данные для помощи в их уголовных расследованиях, что противоречит предыдущим утверждениям, что отслеживание контактов информации будет быть доступна, если пользователь дал положительный результат на вирус.

Это открытие вызвало большой общественный резонанс, при этом некоторые угрожали обойти сбор данных, отключив приложение TraceTogether, отключив Bluetooth-соединение своего телефона или поместив свое устройство, включая токен TraceTogether, в мешочек для блокировки RFID.

Об этой саге уже много сказано, поэтому я не буду ее комментировать дальше, но здесь есть важные уроки для всех, особенно для правительства.

В первую очередь, теперь он должен осознавать, что большие слои местного населения достаточно заботятся о своих личных данных и конфиденциальности и будут защищать их, когда смогут. Это должно послужить сильным сигналом о том, что необходимо серьезное, а не символическое (простите за каламбур) рассмотрение того, как обрабатываются данные граждан, прежде чем развертывать политику.

Совершенно очевидно, что необходимо изменить образ мышления в том, как правительство работает и работает над общенациональными проектами. Для борьбы с пандемией COVID-19 была создана межведомственная целевая группа, при этом усилия по отслеживанию контактов часто занимают центральное место. Тем не менее, прошли месяцы - с момента запуска TraceTogether - без какого-либо министерства или даже полиции, которые, по-видимому, были бы лучше знакомы с Уголовно-процессуальным кодексом, что вызвало тревогу, что неоднократно публичные заявления об использовании отслеживания контактов Данные не учитывали исключения из уголовных расследований.

В худшем случае это может быть воспринято - пусть даже ошибочно - как преднамеренная попытка обмануть общественность. В лучшем случае это будет указывать на грубую небрежность и отсутствие связи между различными министерствами и государственными учреждениями, которым поручено работать над важнейшими национальными инициативами, такими как пандемия COVID-19.

Сага о конфиденциальности TraceTogether дополнительно демонстрирует необходимость для пользователей более сильного владения своими данными, чтобы они могли постоянно задавать вопросы о том, как их личная информация собирается, хранится и используется, а также предпринимать активные шаги для защиты своей собственной кибергигиены.

Потому что, если они этого не сделают, ясно, что не следует ожидать, что бизнес, а также правительство смогут делать это эффективно от их имени. Какие еще лазейки и потенциальные бреши в безопасности были упущены из виду, что потенциально может привести к серьезным нарушениям данных в будущем?

Такие риски можно было бы лучше снизить, если бы пользователи были допущены к усилиям по управлению своими собственными данными и имели

право самостоятельно решать, должны ли компании иметь доступ ко всем или некоторым их личным данным.

Кроме того, каждое объявление о новой политике, предусматривающей доступ к данным граждан, должно сопровождаться информационным бюллетенем о безопасности, в котором подробно описывается, как будет защищаться доступ, а также храниться и защищаться данные. Заявления о необходимости защиты данных должны быть больше, чем на словах, и выходить за рамки коротких одной или двух строк, произносимых просто как попытки «как обычно» решить проблемы безопасности.

«Люди, процессы, технологии». Разве это не основная основа, которую компании и правительства часто называют критически важной для успешного внедрения? Внедрение процессов и технологий ничего не будет значить, если пользователи не будут должным образом оснащены для защиты своих данных». ***(Eileen Yu. Singapore must return data control to users to regain public trust // ZDNet (https://www.zdnet.com/article/singapore-must-return-data-control-to-users-to-regain-public-trust/). 27.01.2021).***

***

«Комиссия по ценным бумагам и инвестициям Австралии (ASIC) заявила, что один из ее серверов был взломан 15 января.

«Этот инцидент связан с программным обеспечением Accellion, используемым ASIC для передачи файлов и вложений», - говорится в сообщении корпоративного регулятора, опубликованном накануне государственного праздника.

«Это включало несанкционированный доступ к серверу, на котором хранились документы, связанные с недавними заявками на получение кредитной лицензии в Австралии».

ASIC заявила, что, хотя была просмотрена некоторая «ограниченная информация», она не обнаружила доказательств того, что какие-либо формы приложений были загружены или открыты. Регулятор сказал, что доступ к серверу был отключен, и он работает над другими механизмами.

«Никакая другая технологическая инфраструктура ASIC не пострадала или не пострадала», - добавил он.

«ASIC работает с Accellion и уведомила соответствующие агентства, а также затронутые стороны, чтобы они отреагировали на инцидент и управляли им».

Accellion также использовался в качестве вектора для взлома Резервного банка Новой Зеландии (RBNZ) в начале этого месяца.

«Сторонний провайдер сообщил нам, что это не была конкретная атака на Резервный банк, и другие пользователи приложения для обмена файлами также были скомпрометированы», - заявили тогда в банке.

В обновлении, опубликованном на прошлой неделе, глава банка Адриан Орр сказал, что причина нарушения «понята и устранена».

«На основе результатов нашего расследования и анализа на сегодняшний день мы смогли сообщить заинтересованным сторонам, какие из их файлов в

приложении для передачи файлов были загружены незаконно во время взлома», - сказал он.

«Есть несколько серьезных вопросов, на которые ответила команда в Банке, и есть другие вопросы к поставщику системы, которая была взломана. Это предмет независимой проверки KPMG, которая в настоящее время проводится».

РБНЗ заявил, что уже находится в процессе внедрения новой системы безопасной передачи файлов для использования с внешними заинтересованными сторонами, и что работа была ускорена.

Со своей стороны, Accellion заявила 12 января, что она знала об уязвимости в своем устаревшем приложении для передачи файлов с середины декабря и выпустила исправление за 72 часа для «менее чем 50 затронутых клиентов».

«Accellion FTA - это продукт 20-летней давности, который специализируется на передаче больших файлов», - говорится в сообщении.

«В то время как Accellion поддерживает строгие стандарты безопасности для своего устаревшего продукта FTA, мы настоятельно рекомендуем нашим клиентам перейти на kiteworks, современную платформу межсетевого экрана корпоративного контента, чтобы обеспечить высочайший уровень безопасности и уверенности». ***(Chris Duckett. ASIC reports server breached via Accellion vulnerability // ZDNet (https://www.zdnet.com/article/asic-reports-server-breached-via-accellion-vulnerability/). 27.01.2021).***

***

«Управление австралийского комиссара по информации (OAIC) приказало Министерству внутренних дел, бывшему Департаменту иммиграции и охраны границ, определить сумму, причитающуюся каждому человеку, и выплатить компенсацию за «ошибочное» раскрытие личной информации 9 251 просителя убежища.

Комиссар Австралии по вопросам информации и конфиденциальности Анджелина Фальк определила, что федеральное правительство в то время «вмешалось» в частную жизнь этих людей, случайно опубликовав их полные имена, национальность, местонахождение, даты прибытия и информацию о прибытии лодок на своем веб-сайте. в 2014.

После публикации своей личной информации лица, ищущие убежища, возбудили иск против ведомства. Соискатели убежища в Новом Южном Уэльсе, Западной Австралии и Северной территории утверждали, что нарушение подвергло их преследованию со стороны властей в их странах.

В рамках судебного дела было подано 1297 заявлений о выплате компенсации, поскольку пострадавшие понесли убытки или ущерб из-за утечки данных.

Комиссар сказал, что компенсация, которая будет выплачиваться участвующим ученикам, будет варьироваться от 500 австралийских долларов до более чем 20 000 долларов и будет определяться в каждом конкретном случае.

«Это первое представительное действие, в котором мы нашли компенсацию за неэкономический ущерб, выплачиваемую лицам, пострадавшим от утечки данных», - сказала она.

«Он признает, что потеря конфиденциальности или раскрытие личной информации может повлиять на людей и, в зависимости от обстоятельств, вызвать убытки или ущерб».

Ожидается, что процесс компенсации займет до 12 месяцев. Это будет включать обеспечение того, чтобы люди соглашались на сумму компенсации. OAIC сообщила, что если департамент и физическое лицо не могут договориться о сумме компенсации, появится возможность пересмотреть сумму, подлежащую выплате.

OAIC заявила, что также опубликует информацию о решении на 21 языке, чтобы все участвующие члены класса были проинформированы о процессе, чтобы они могли завершить свои требования.

На прошлой неделе OAIC обратилось с просьбой о внесении поправок в Закон о конфиденциальности 1988 года, которые обновят его регулирующие полномочия и отменит исключения, например, для политических партий.

В 150-страничном представлении [PDF] для обзора Закона Генеральным прокурором OAIC внесла несколько рекомендаций, в том числе о расширении собственных возможностей регулирования, которые, по его словам, приведут его полномочия в соответствие с «ожиданиями сообщества».

Действующий Закон о конфиденциальности позволяет регулирующему органу разрешать индивидуальные жалобы на нарушение конфиденциальности путем переговоров, примирения и принятия решений. OAIC охарактеризовал эту функцию, которой почти 33 года, как устаревшую.

"Это отражает контекст, в котором впервые был введен Закон о конфиденциальности. В цифровой среде ущерб конфиденциальности может возникать в более широком масштабе. Хотя рассмотрение индивидуальных жалоб является необходимой частью эффективного регулирования конфиденциальности, должно быть больше возможностей для проведения значительных риски конфиденциальности и систематическое несоблюдение нормативных требований», - говорится в сообщении.

«В то время как текущая структура Австралии предоставляет некоторые правоприменительные полномочия, их необходимо усилить и перенастроить, чтобы сдерживать несоответствующее поведение и гарантировать исправление практики». ***(Aimee Chanthadavong. OAIC orders Home Affairs to compensate asylum seekers over data breach // ZDNet (https://www.zdnet.com/article/oaic-orders-home-affairs-to-compensate-asylum-seekers-over-data-breach/). 27.01.2021).***

***

«Если ваш выбор между приложениями для обмена зашифрованными сообщениями - это выбор между Signal, Telegram и WhatsApp, не тратьте свое время ни на что, кроме Signal. Дело не в том, что имеет более симпатичные функции, больше наворотов или наиболее удобно в использовании - речь идет о чистой конфиденциальности. Если это то, что вам нужно, ничто не сравнится с Signal.

К настоящему времени вы, вероятно, уже знаете, что произошло. 7 января в твите, разнесенном по всему миру, технический магнат Илон Маск продолжил

свою вражду с Facebook, призывая людей отказаться от его мессенджера WhatsApp и использовать Signal. Генеральный директор Twitter Джек Дорси ретвитнул свой звонок. Примерно в то же время правая социальная сеть Parler закрылась после атак на Капитолий, а политические бойкоты покинули Facebook и Twitter. Это был идеальный шторм - с тех пор количество новых пользователей Signal и Telegram выросло на десятки миллионов.

Эта встряска также привела к более широкой проверке безопасности и конфиденциальности приложений для обмена сообщениями. Среди трех доминирующих в настоящее время цифр загрузок есть некоторые общие черты. Все три являются мобильными приложениями, доступными в Play Store и App Store, которые поддерживают межплатформенный обмен сообщениями, имеют функции группового чата, предлагают многофакторную аутентификацию и могут использоваться для обмена файлами и фотографиями. Все они обеспечивают шифрование текстовых, голосовых и видеозвонков.

Signal, Telegram и WhatsApp используют сквозное шифрование в некоторых частях своего приложения, а это означает, что если посторонняя сторона перехватит ваши тексты, они должны быть зашифрованы и нечитаемы. Это также означает, что точное содержание ваших сообщений якобы не может быть просмотрено людьми, работающими в любом из этих приложений, когда вы общаетесь с другим частным пользователем. Это не позволяет правоохранительным органам, вашему оператору мобильной связи и другим отслеживающим лицам читать содержимое ваших сообщений, даже если они их перехватывают (что происходит чаще, чем вы думаете).

Однако различия в конфиденциальности и безопасности между Signal, Telegram и WhatsApp не могут быть больше. Вот что вам нужно знать о каждом из них.

Signal

Не собирает данные, только ваш номер телефона

Бесплатно, без рекламы, финансируется некоммерческой организацией Signal Foundation

Полностью открытый исходный код

Шифрование: протокол сигнала

Signal - это типичное приложение для установки в одно касание, которое можно найти на обычных торговых площадках, таких как Google Play Store и Apple App Store, и оно работает так же, как обычное приложение для обмена текстовыми сообщениями. Это разработка с открытым исходным кодом, бесплатно предоставляемая некоммерческой организацией Signal Foundation, и на протяжении многих лет она широко использовалась известными иконами конфиденциальности, такими как Эдвард Сноуден.

Основная функция Signal заключается в том, что он может отправлять - как отдельному лицу, так и группе - полностью зашифрованные текстовые, видео, аудио и графические сообщения после проверки вашего номера телефона и позволяя вам независимо проверять личность других пользователей Signal. Чтобы глубже погрузиться в потенциальные ловушки и ограничения приложений для

зашифрованного обмена сообщениями, вам поможет объяснитель Лоры Хаутала из CNET.

Когда дело доходит до конфиденциальности, трудно превзойти предложение Signal. Он не хранит ваши пользовательские данные. Помимо возможностей шифрования, он предоставляет расширенные параметры конфиденциальности на экране, включая блокировку приложений, пустые всплывающие окна с уведомлениями, средства защиты от слежки с размытием лица и исчезающие сообщения.

Случайные ошибки доказали, что эта технология, конечно, далека от пуленепробиваемости, но общая репутация и результаты Signal удерживают ее в верхней части списка инструментов защиты личных данных каждого разбирающегося в конфиденциальности человека. The Guardian, The Washington Post, The New York Times (которая также рекомендует WhatsApp) и The Wall Street Journal - все они рекомендуют использовать Signal для безопасного общения со своими репортерами.

В течение многих лет основная проблема конфиденциальности для Signal заключалась не в технологиях, а в их более широком распространении. Отправка зашифрованного сообщения Signal - это прекрасно, но если ваш получатель не использует Signal, ваша конфиденциальность может быть нулевой. Думайте об этом как о коллективном иммунитете, создаваемом вакцинами, но для конфиденциальности ваших сообщений.

Однако теперь, когда одобрение Маска и Дорси направило поток пользователей, желающих повысить конфиденциальность, эта проблема может остаться в прошлом.

Telegram

Связанные с вами данные: имя, номер телефона, контакты, идентификатор пользователя.

Предстоящая бесплатная рекламная платформа и премиум-функции, финансируемые главным образом основателем

Только частично с открытым исходным кодом

Шифрование: MTProto

Telegram находится где-то в середине шкалы конфиденциальности, и он стоит особняком от других приложений для обмена сообщениями из-за его усилий по созданию среды в стиле социальных сетей. Хотя он не собирает столько данных, сколько WhatsApp, он также не предлагает зашифрованные групповые вызовы, такие как WhatsApp, а также не обеспечивает такую конфиденциальность данных пользователей и прозрачность компании, как Signal. Данные, собранные Telegram, которые могут быть связаны с вами, включают ваше имя, номер телефона, список контактов и идентификатор пользователя.

Telegram также собирает ваш IP-адрес, чего еще не делает Signal. И в отличие от Signal и WhatsApp, индивидуальные сообщения Telegram по умолчанию не шифруются. Скорее, вы должны включить их в настройках приложения. Групповые сообщения Telegram также не зашифрованы. Исследователи обнаружили, что, хотя некоторые схемы шифрования MTProto в Telegram были с

открытым исходным кодом, некоторые части - нет, поэтому не совсем понятно, что происходит с вашими текстами, когда они находятся на серверах Telegram.

Telegram видел несколько нарушений. Около 42 миллионов идентификаторов пользователей и номеров телефонов Telegram были раскрыты в марте 2020 года, что считается делом работы иранских правительственных чиновников. Это будет второе крупное нарушение, связанное с Ираном, после того, как в 2016 году было обнаружено 15 миллионов иранских пользователей. В 2019 году власти Китая использовали ошибку Telegram во время протестов в Гонконге. Затем был бот в Telegram, которому разрешили создавать поддельные обнаженные женщины из обычных фотографий. Совсем недавно его функция с поддержкой GPS, позволяющая вам находить других рядом с вами, создала очевидные проблемы для конфиденциальности.

Я связался с Telegram, чтобы узнать, разрабатываются ли какие-либо серьезные планы безопасности для приложения, и каковы были его приоритеты безопасности после этого последнего всплеска количества пользователей. Я обновлю эту историю, когда получу ответ.

WhatsApp

Связанные с вами данные: слишком много, чтобы перечислить (см. Ниже)

Свободный; бизнес-версии доступны бесплатно, финансируются Facebook

Не с открытым исходным кодом, кроме шифрования

Шифрование: протокол сигнала

Давайте проясним: есть разница между безопасностью и конфиденциальностью. Безопасность - это защита ваших данных от несанкционированного доступа, а конфиденциальность - это защита вашей личности независимо от того, кто имеет доступ к этим данным.

Что касается безопасности, шифрование WhatsApp такое же, как и в Signal, и это шифрование является безопасным. Но этот протокол шифрования - одна из немногих частей WhatsApp с открытым исходным кодом, поэтому нас просят доверять WhatsApp больше, чем нам Signal. Фактическое приложение WhatsApp и другая инфраструктура также подвергались взломам, как и Telegram.

В январе 2020 года телефон Джеффа Безоса был взломан с помощью видеосообщения в WhatsApp. В декабре того же года генеральный прокурор Техаса заявил - хотя это не доказало - что Facebook и Google заключили закулисную сделку по раскрытию содержания сообщений WhatsApp. Поставщик шпионского ПО нацелился на уязвимость WhatsApp с помощью своего программного обеспечения, чтобы взломать 1400 устройств, в результате чего Facebook подал в суд. Функция незашифрованного облачного резервного копирования в WhatsApp долгое время считалась угрозой безопасности экспертами по конфиденциальности и была одним из способов, которыми ФБР получило доказательства на печально известного политолога Пола Манафорта. В довершение всего, WhatsApp также стал известен как рай для мошенников и распространителей вредоносных программ. на протяжении многих лет (точно так же, как Telegram привлек свою долю злоупотреблений платформой, как описано выше).

Несмотря на взломы, в WhatsApp меня беспокоит не столько аспект безопасности, сколько конфиденциальность. Я не горю желанием, чтобы Facebook

установил на моем телефоне еще одну программу, с которой он может получать еще больше поведенческих данных с помощью простого в использовании приложения с красивым интерфейсом и большей безопасностью, чем в обычном мессенджере.

Когда WhatsApp сообщает, что не может просматривать содержимое зашифрованных сообщений, которые вы отправляете другому пользователю WhatsApp, это не говорит о том, что существует обширный список других данных, которые он собирает, которые могут быть связаны с вашей личностью: ваше уникальное устройство Идентификационные данные, данные об использовании и рекламе, история покупок и финансовая информация, физическое местоположение, номер телефона, ваша контактная информация и информация из вашего списка контактов, с какими продуктами вы взаимодействовали, как часто вы используете приложение и как оно работает, когда ты сделаешь. Этот список можно продолжить. Это намного больше, чем Signal или Telegram.

Когда я спросил компанию, почему пользователи должны соглашаться на меньшую конфиденциальность данных, представитель WhatsApp указал, что она ограничивает то, что она делает с этими пользовательскими данными, и что сбор данных применяется только к некоторым пользователям. Например, сбор данных о финансовых транзакциях будет актуален только для тех пользователей WhatsApp в Бразилии, где доступна эта услуга.

«Мы не передаем ваши контакты в Facebook, и мы не можем видеть ваше общее местоположение», - сказал CNET представитель WhatsApp.

«Хотя большинство людей используют WhatsApp только для общения с друзьями и семьей, мы также начали предлагать людям возможность общаться в чате с представителями бизнеса, чтобы получить помощь или совершить покупку, с органами здравоохранения, чтобы получить информацию о COVID, с поддержкой по вопросам домашнего насилия. агентства, а также службы проверки фактов, чтобы предоставить людям возможность получать точную информацию», - сказал представитель. «По мере расширения наших услуг мы продолжаем защищать сообщения людей и ограничивать информацию, которую мы собираем».

WhatsApp удобнее Signal и Telegram? Да. Это красивее? Конечно. Это так же безопасно? Мы не узнаем, если не увидим больше его исходного кода. Но разве это более личное? Не когда дело доходит до того, сколько данных он собирает сравнительно. Для настоящей конфиденциальности я придерживаюсь Signal и рекомендую вам сделать то же самое». ***(Rae Hodge. Signal vs. WhatsApp vs. Telegram: Here's which secure messaging app to use // CNET (https://www.cnet.com/news/signal-vs-whatsapp-vs-telegram-heres-which-secure-messaging-app-to-use/?ftag=CAD090e536&bhid=20102274281679224800074149012732&mid=13242216&cid=534816904). 25.01.2021).***

***

«Магазин мужской одежды Bonobos подвергся серьезной утечке данных, в результате чего была раскрыта личная информация миллионов клиентов после того, как злоумышленник загрузил облачную резервную копию их базы

данных. Бонобо заявляет, что во время атаки взлом корпоративных систем не происходил.

Bonobos начинал как интернет-магазин мужской одежды, но позже расширился до шестидесяти мест, где можно было примерить одежду перед покупкой. Walmart купил Bonobos в 2017 году за 300 миллионов долларов, чтобы продавать свою одежду на своем сайте Jet.com.

В минувшие выходные злоумышленник, известный как ShinyHunters, известный взломом онлайн-сервисов и продажей украденных баз данных, разместил полную базу данных Bonobos на бесплатном хакерском форуме.

Утечка огромной базы данных объемом 70 ГБ

Эта просочившаяся база данных представляет собой огромный SQL-файл объемом 70 ГБ, содержащий различные внутренние таблицы, используемые веб-сайтом Bonobos. База данных также включает различные данные, гораздо более интересные для злоумышленников, такие как адреса клиентов, номера телефонов, частичные номера кредитных карт (последние четыре цифры), информацию о заказах, истории паролей.

Количество записей зависит от категории данных. Например, адрес и номера телефонов предназначены для 7 миллионов клиентов / заказов, информация о счете для 1,8 миллиона зарегистрированных клиентов и 3,5 миллиона частичных записей по кредитным картам.

Пароли, хранящиеся в базе данных, хешируются с использованием SHA-256 или SHA-512 в зависимости от злоумышленников, которые начали анализ базы данных. Один злоумышленник утверждает, что уже взломал пароли для 158 000 паролей SHA-256, но не смог взломать пароли SHA-512.

Хакер превратил взломанные пароли в «комболист», используемый в атаках с заполнением учетных данных, то есть для входа в систему с использованием украденных учетных данных на других сайтах.

База данных резервного копирования была украдена из облака

…магазин одежды сообщил, что злоумышленники получили доступ не к внутренним системам, а к файлу резервной копии, размещенному во внешней облачной среде.

«Мы очень серьезно относимся к защите данных наших клиентов. Мы продолжаем расследование этого вопроса и пока не обнаружили никаких доказательств того, что неавторизованные стороны получали доступ к внутренней системе Bonobos. Мы обнаружили, что неавторизованная третья сторона была возможность просматривать файл резервной копии, размещенный во внешней облачной среде. Мы связались с провайдером хоста, чтобы решить эту проблему, как только нам стало известно о ней».

«Кроме того, мы предприняли дополнительные меры предосторожности, в том числе отключение точек доступа, аннулирование паролей учетных записей и требование сброса паролей, чтобы еще больше обезопасить учетные записи клиентов. Мы отправляем клиентам электронное письмо с уведомлением о том, что их контактная информация и зашифрованные пароли могли быть просмотрены неавторизованной третьей стороной. Эта проблема не повлияла на платежную

информацию. Мы будем продолжать делиться обновлениями с клиентами по мере их появления», - сказал Бонобос BleepingComputer по электронной почте.

Хотя база данных не включала в себя полную информацию о платежах, злоумышленники могут использовать частичные данные в целевых фишинговых атаках…». ***(Lawrence Abrams. Bonobos clothing store suffers a data breach, hacker leaks 70GB database // Bleeping Computer (https://www.bleepingcomputer.com/news/security/bonobos-clothing-store-suffers-a-data-breach-hacker-leaks-70gb-database/). 22.01.2021).***

***

«Личные данные 66 000 пользователей были оставлены открытыми на неправильно настроенном сервере Elasticsearch, что пополнило список компаний с дырявыми облаками.

VIPGames.com, бесплатная платформа с 56 доступными классическими настольными и карточными играми, такими как Hearts, Crazy Eights, Euchre, Dominoes, Backgammon и другими, раскрыла личные данные десятков тысяч пользователей.

В целом, согласно новому отчету WizCase, более 23 миллионов записей для более чем 66 000 пользователей остались открытыми из-за неправильной конфигурации облака. Помимо пользователей настольных компьютеров, у VIPGames есть и мобильные плееры, в том числе через приложение, которое было загружено из магазина Google Play только более 100 000 раз.

Сайт пополнил растущий список компаний, уличенных в отсутствии правильно настроенных облаков, что может привести к плачевным результатам для клиентов.

Исследовательская группа WizCase, возглавляемая Атой Хаклом, регулярно сканирует Интернет на предмет открытых серверов и обнаруживает, что конфиденциальная личная информация открыта и доступна любому киберпреступнику, который случайно наткнется на нее.

В отчете поясняется, что онлайн-игры представляют собой особенно желательный набор личных данных для киберпреступников.

Дырявые облака для геймеров особенно опасны

«Онлайн-игры объединяют личную информацию пользователей, детали транзакций и игровые привычки. Такое сочетание конфиденциальной информации создает выгодную среду для использования киберпреступниками», - поясняется в отчете WizCase. «Игровые платформы регулярно подвергаются многочисленным атакам со стороны хакеров, саботажу со стороны конкурирующих платформ, внутриплатформенным атакам игроков, нацеленных на интернет-соединения конкурирующих пользователей, и многому другому».

В этом случае с незащищенного сервера сайта произошла утечка более 30 ГБ данных, содержащих 23 миллиона отдельных записей, включая имена пользователей, электронные письма, IP-адреса, хешированные пароли, идентификаторы Facebook, Twitter и Google, ставки и даже данные об игроках, которым запрещен доступ к платформе., - сказал WizCase.

«Каждый из этих наборов данных не только ценен сам по себе, но также может использоваться для отображения другой информации», - поясняется в отчете. «Например, по идентификаторам игроков злоумышленник может найти адрес электронной почты, IP-адрес и хешированный пароль игрока, что особенно актуально для заблокированных игроков».

В отчете добавлено, что Условия использования VIPGames.com объясняют, что игроки могут быть заблокированы на платформе за плохое поведение или обман, и что открытые записи включают грязные детали каждого нарушения.

«Некоторые из них включают потенциальную педофилию и эксгибиционизм», - сказал WizCase, добавив потенциальный шантаж к списку угроз, представляемых открытыми данными для пользователей, помимо кражи личных данных, взлома паролей, фишинга, вредоносных программ и многого другого.

Threatpost обратился к VIPGames.com за комментарием, но не получил ответа.

И хотя это нарушение вызывает тревогу, оно является частью более широкой тенденции компаний, которые не могут заблокировать свои данные в облаке.

Неправильно настроенные облака повсюду

В сентябре прошлого года компания Razer, производящая высококачественное игровое оборудование, оставила личные данные около 100 000 пользователей открытыми в аналогичном облачном кластере Elasticsearch.

В том же месяце было обнаружено, что группа из 70 различных сайтов знакомств для взрослых хранит конфиденциальные личные данные, такие как сексуальные предпочтения, на незащищенном сервере Elasticsearch, в результате чего произошла утечка более 320 миллионов индивидуальных записей.

В апреле приложение цифрового кошелька Key Ring показало 44 миллиона записей клиентов, включая идентификаторы, платежные карты, карты лояльности, подарочные карты и членские карты, оставленные открытыми на сервере Amazon Web Services S3. А прошлым летом Joomla опубликовала данные 2700 человек, подписавшихся на форум сообщества Joomla Resources Directory в незащищенном облачном хранилище Amazon Web Services.

По оценкам подразделения 42 Palo Alto Networks, около 60 процентов взломов происходит из-за неправильно настроенных публичных облаков.

Райан Олсон, вице-президент по анализу угроз в группе Unit 42, объяснил, что, хотя 86 процентов компаний развертывают облачные приложения, только 34 процента имеют «решения единого входа» (SSO), демонстрируя огромный пробел в внедрении облачных и необходимых решения для облачной безопасности».

Что касается пользователей, эксперты согласны с тем, что основные передовые методы обеспечения онлайн-безопасности всегда являются хорошей идеей - будьте осторожны с тем, чем вы делитесь, избегайте нажатия на подозрительные электронные письма или ссылки, и правильная гигиена паролей важны, советует WizCase. Фирма также предложила использовать VPN-сервис для защиты данных о местоположении и установить хорошее антивирусное программное обеспечение, в то время как отрасль пытается не отставать.

«Использование облака позволяет организациям легко достигать своих целей и масштабироваться», - сказал Анураг Кахол, технический директор Bitglass, по электронной почте. «По мере того как все больше организаций внедряют облачные инструменты для получения конкурентного преимущества, темпы использования облачных приложений возрастают одновременно. Однако большинство организаций не в состоянии удовлетворить требования безопасности облака». ***(Becky Bracken. 23M Gamer Records Exposed in VIPGames Leak // Threatpost (https://threatpost.com/gamer-records-exposed-vipgames-leak/163352/). 26.01.2021).***

***

«В округе Кук, штат Иллинойс, где проживает Чикаго, с сентября была открыта база данных, содержащая конфиденциальные данные уголовного и семейного суда.

По словам исследователей, незащищенная паролем база данных, принадлежащая округу в Иллинойсе, выявила 323 000 судебных записей в течение как минимум четырех месяцев. База данных выявила имена различных лиц, вовлеченных в деликатные уголовные дела, дела о домашнем насилии или опеке над детьми.

Исследователи из Website Planet (совместно с исследователем безопасности Джереми Фаулером) утверждали, что база данных принадлежит округу Кук, где проживает город Чикаго, и в котором проживает 5,1 миллиона человек (что делает его вторым по численности населения округом в США после округа Лос-Анджелес.).

Исследователи обнаружили базу данных 26 сентября и вскоре после этого уведомили технического директора округа Кук о разоблачении. Однако база данных оставалась открытой до понедельника на этой неделе, когда она была защищена и публичный доступ был ограничен.

«Почти каждая запись содержала ту или иную форму личной информации (PII), такой как полные имена, домашние адреса, адреса электронной почты, номера дел и личные данные о делах», - заявили исследователи из Website Planet во вторник. «На основании раскрытой потенциально конфиденциальной информации стало ясно, что эти данные не предназначались для публикации».

База данных представляла собой внутреннюю систему управления записями, содержащую подробные данные о статусе или проблемах с различными делами.

Неясно, какая конкретная часть округа управляла базой данных (Threatpost обратился к Website Planet для дальнейших комментариев). На веб-сайте округа Кук указано, что клерк окружного суда отвечает за ведение судебных материалов и архивов, а также за помощь в содержании детей, записи о разводе и судебные электронные дела.

Обнародованные судебные протоколы, датированные периодом с 2012 по 2020 год, раскрыли как истцов, так и ответчиков «в тоне, который явно был предназначен только для внутреннего использования и не должен был разглашаться публично», говорят исследователи.

В базе данных были файлы с пометкой «IMM», которые исследователи считали различными записями иммиграционного суда; включая различные адреса

электронной почты (связанные с учетными записями USCIS, которые используются для служб гражданства и иммиграции) и различные судебные записи, включающие имена, номера дел и заметки о статусе или ходе рассмотрения дела (например, если клиенту нужен переводчик).

Исследователи полагают, что эти судебные документы принадлежали специализированному отделу или работникам судов округа Кук, которые помогали тем, кто не говорил по-английски или нуждался в какой-либо помощи суда.

Также частью базы данных были различные записи уголовных судов (обозначенные CRI) и дела судов по семейным делам (обозначенные FAM). Это могут быть дела, касающиеся развода (включая опеку над детьми и посещения), домашнего насилия, Отдела защиты детей (который занимается защитой несовершеннолетних от жестокого обращения) и Отдел ювенальной юстиции (который занимается преступлениями несовершеннолетних).

Вердикт: возможны большие кибератаки

Исследователи заявили, что при доступе к этой базе злоумышленников она станет «золотой жилой» для целевого фишинга и фишинговых кампаний, шантажа, кражи личных данных и других гнусных действий.

Например, мошенники могут нацеливаться на иммигрантов, чья личная информация была частью базы данных, угрожая депортацией, если не будет уплачен выкуп. Они также могли шантажировать семьи тем, что они могут утечь их личную информацию, касающуюся развода или домашнего насилия, если выкуп не будет выплачен.

Незащищенные базы данных по-прежнему раскрывают различные типы конфиденциальной информации в Интернете. Ранее в январе неправильно настроенная база данных ElasticSearch предоставила более 400 ГБ данных общедоступных и частных профилей для 214 миллионов пользователей социальных сетей со всего мира, включая информацию о знаменитостях и влиятельных лицах в социальных сетях в США и других странах. А в сентябре неправильная конфигурация облака в магазине игрового оборудования Razer потенциально подвергла 100 000 клиентов фишингу и мошенничеству…». ***(Lindsey O'Donnell. Criminal, Domestic Violence Case Info Exposed in Cook County Leak // Threatpost (https://threatpost.com/criminal-domestic-case-cook-county-leak23k-sensitive-court-records/163336/). 26.01.2021).***

***

«Експерти закликають бути дуже обережними з оприлюдненням персональних даних - навіть після їх видалення Ви не можете гарантувати, що ці дані не були збережені іншими особами або ресурсами.

Сьогодні, 28 січня світ святкує Міжнародний день захисту персональних даних та 40 річницю Конвенції Ради Європи про захист осіб у зв’язку з автоматизованою обробкою персональних даних…

Якими законодавчими актами регламентується захист персональних даних в Україні?

Відповідає Олег Заярний, експерт спільного проєкту «Європейський Союз та Рада Європи працюють разом задля посилення операційної спроможності Омбудсмана у захисті прав людини»

В Україні стандарти правового регулювання відносин щодо обробки та захисту персональних даних закладені такими актами Ради Європи, як: Конвенція про захист прав людини і основоположних свобод, а також Конвенція № 108 про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних.

Крім згаданих міжнародно-правових актів, у нашій Державі відносини щодо обробки і захисту персональних даних регламентуються нормами Конституції України, зокрема статті 32, Законом України «Про захист персональних даних», іншими законами України та підзаконними актами, якими визначаються особливості обробки і захисту в окремих сферах суспільної діяльності.

Який орган в Україні відповідає за захист персональних даних?

Відповідає Олег Заярний, експерт спільного проєкту «Європейський Союз та Рада Європи працюють разом задля посилення операційної спроможності Омбудсмана у захисті прав людини»

Державним органом, відповідальним в Україні за забезпечення захисту персональних даних є Уповноважений Верховної Ради України з прав людини.

Саме до Уповноваженого подаються скарги на рішення, дії чи бездіяльність володільців і розпорядників персональних даних, повідомлення про початок обробки персональних даних, що становить особливий ризик для прав суб'єктів персональних даних.

Уповноважений Верховної Ради України наділений повноваженнями щодо проведення перевірок діяльності володільців та розпорядників персональних даних, складати протоколи про адміністративні правопорушення у сфері обробки персональних даних, направляти відповідні матеріали до суду з метою притягнення винних осіб до адміністративної відповідальності.

Цей державний орган здійснює не лише контрольно-наглядові повноваження. Уповноважений Верховної Ради України з прав людини проводить також моніторинг додержання законодавства про захист персональних даних по всій території України, здійснює широку просвітницьку кампанію у цій сфері, взаємодіє з наглядовими органами інших держав з питань обробки і захисту персональних даних…» ***(Як захистити свої персональні дані в інтернеті? Відповідають експерти Ради Європи // MediaSapiens (https://ms.detector.media/trendi/post/26505/2021-01-28-yak-zakhystyty-svoi-personalni-dani-v-interneti-vidpovidayut-eksperty-rady-yevropy/). 28.01.2021).***

***

«Сотрудникам Citrix, которые стали жертвами утечки данных, выплатят $2,3 млн.

На днях это предложение было одобрено судьей.

Коллективный иск, включавший примерно 24,300 человек, будет урегулирован выплатой компанией суммы в размере $2,3 млн. Деньги пойдут на услуги мониторинга, восстановление украденных ID и выплаты каждому в размере до $15,000.

Citrix раскрыла утечку в мае 2019 года после того, как ФБР сообщило им о возможном вторжении. Киберпреступники могли подключаться к серверам компании около 5 месяцев между 2018 и 2019 годами.

Компания сообщила, что злоумышленники периодически имели доступ к корпоративным ресурсам, который они получали методом password spraying - распространенный способ скомпрометировать как личные, так и корпоративные аккаунты.

Слушание назначено на 10 июня 2021 года. В этот день урегулирование может быть завершено». ***(Одобрено предложение Citrix о выплате $2,3 млн сотрудникам, которые стали жертвами утечки данных // SecureNews (https://securenews.ru/citrixs-offer-to-pay-2-3-million-to-employees-who-were-victims-of-a-data-breach-has-been-approved/). 28.01.2021).***

***

«Шахраї придбали базу даних з телефонними номерами користувачів Facebook, тепер ці дані продають за допомогою бота в Telegram…

За словами дослідника з питань кібербезпеки Алона Гала, творець бота, стверджує, що у нього є інформація про 533 мільйонів користувачів, отримана через уразливість Facebook, яка була виправлена в 2019 році.

Бот, по даним видання, дозволяє бажаючим робити дві речі: якщо у людини є ідентифікатор користувача Facebook, він може знайти номер телефону цієї людини, а якщо у нього є номер телефону, він може знайти його ідентифікатор користувача Facebook.

Отримання доступу до інформації коштує грошей — розблокування частини інформації на зразок телефонних номерів телефону або ідентифікатора Facebook, автор бота продає за 20 доларів.

Згідно скріншотам, опублікованими Галом, бот працює як мінімум з 12 січня 2021 року, але дані, до яких він надає доступ, відносяться до 2019 року…» ***(Саша Картер. Номери 533 мільйонів користувачів Facebook продаються у Telegram з допомогою бота // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1913987-nomera-533-milyoniv-koristuvachiv-facebook-prodayutsya-u-telegram-z-dopomogoyu-bota). 26.01.2021).***

***

Кібербезпека Інтернету речей

«В декабре 2020 года президент Трамп подписал двухпартийный закон, который устанавливает стандарты безопасности для федеральных покупок устройств, подключенных к Интернету. Этот закон, Закон о совершенствовании кибербезопасности IoT (Закон), устанавливает новые национальные правила, регулирующие растущий рынок технологий промышленного Интернета вещей (IoT). Закон требует от Национального института стандартов и технологий разработки минимальных стандартов кибербезопасности для любого

подключенного к Интернету устройства, продаваемого поставщиками правительству США. От этих поставщиков Интернета вещей также требуется разработать политики раскрытия уязвимостей, которые позволят федеральным чиновникам узнавать о недостатках безопасности, как только они обнаруживаются.

Как законопроект, закон прошел через Палату представителей и Сенат при подавляющей поддержке. Ни один сенатор не возражал против его одобрения и не добивался поименного голосования в ноябре 2020 года. Как закон, Закон будет защищать национальную безопасность и личную информацию американских семей, гарантируя, что правительство США закупит безопасные технологические устройства и устранит существующие уязвимости. Федеральные устройства, подключенные к Интернету, могут включать в себя различные системы, такие как лифты, системы пожаротушения, обогрев и охлаждение, освещение, аудио- и видеооборудование и, в конечном итоге, автономные транспортные средства.

До принятия закона правительство США закупало устройства Интернета вещей без стандартов безопасности, чтобы предотвратить их использование в атаках или получение несанкционированных точек доступа к правительственным сетям США. Теперь наша федеральная инфраструктура более защищена от угроз, как внешних, так и внутренних. Закон, получивший поддержку со стороны таких тяжеловесов отрасли, как The Software Alliance, устанавливает первые федеральные стандарты для быстрорастущего мира технологий, который, по оценкам, достиг 20,4 миллиарда единиц устройств. Более того, производители устройств IoT приветствуют четкие национальные стандарты, которые, вероятно, выйдут за рамки федеральных контрактов и будут регулировать области, касающиеся того, как эти устройства создаются для населения…

Закон о совершенствовании кибербезопасности IoT - это только первый шаг к повышению безопасности устройств IoT, и несколько штатов даже начали принимать местное законодательство, обеспечивающее регулирование и в этой растущей отрасли. Команда Броуса Макдауэлла по кибербезопасности и конфиденциальности данных может предоставить рекомендации и инструменты, необходимые для навигации по правилам Интернета вещей и другим законам о безопасности и конфиденциальности данных. Наряду с предоставлением вашему бизнесу информации о соблюдении законодательства о конфиденциальности, мы также предоставляем компаниям проактивные решения для защиты от кибератак и общие рекомендации по всем сложностям всех законов и постановлений о конфиденциальности данных. Наша команда предлагает широкий спектр услуг, в том числе планирование до взлома и кибербезопасности, транзакционные услуги кибербезопасности и конфиденциальности данных, услуги по обеспечению соответствия нормативным требованиям, услуги по реагированию на нарушения и раскрытие информации, обзор страхования кибербезопасности и любые связанные с этим судебные вопросы, касающиеся кибербезопасности и утечки данных (расследование, защита, страховое возмещение и реагирование). Свяжитесь с нами, чтобы получить дополнительную информацию и узнать, как мы можем сотрудничать с вами». ***(Jarman J. Smith. Cybersecurity Alert: IoT Security Bill is Signed Into Law // Brouse McDowell (https://www.brouse.com/cybersecurity-alert-iot-security-bill-is-signed-into-law). 07.01.2021).***

***

«Национальный институт стандартов и технологий (NIST) в течение нескольких лет был активным двигателем усилий по обеспечению кибербезопасности Интернета вещей (IoT), собирая заинтересованные стороны из федерального правительства и частного сектора для разработки руководства по управлению рисками IoT. На сегодняшний день программа NIST Cybersecurity for IoT Program объединилась в рамках широкой экосистемы IoT для разработки основополагающих добровольных рекомендаций, включая Базовый уровень возможностей кибербезопасности устройств IoT, который определяет набор возможностей кибербезопасности устройств, которые организации должны учитывать при управлении рисками IoT.

Важная работа NIST в области безопасности Интернета вещей будет продолжена в 2021 году. Последние события, в том числе принятие Закона о повышении кибербезопасности Интернета вещей (IoT) 2020 года (Закон об улучшении кибербезопасности Интернета вещей) и недавно выпущенный список проектов руководящих документов - обещание впереди NIST год, а также множество возможностей для продолжения работы в отрасли.

Закон о совершенствовании кибербезопасности Интернета вещей требует от NIST разработать минимальные стандарты безопасности и руководящие принципы для федерального правительства, которые лягут в основу новых ограничений на закупки.

4 декабря 2020 г. был подписан двухпартийный Закон о повышении уровня кибербезопасности Интернета вещей. Новый закон требует базовых стандартов безопасности и руководящих принципов для устройств Интернета вещей, принадлежащих или контролируемых федеральными правительственными учреждениями. В частности, закон требует от NIST разрабатывать и публиковать для федерального правительства стандарты и руководства по надлежащему использованию и управлению устройствами IoT агентствами, включая минимальные требования безопасности. Основываясь на этих стандартах и рекомендациях, Управление управления и бюджета (OMB), в консультации с NIST и Министерством внутренней безопасности США (DHS), должно пересмотреть политики и принципы информационной безопасности IoT федеральных агентств, а также опубликовать политики и принципы в качестве необходимо - для обеспечения соответствия стандартам и рекомендациям NIST. В дополнение к положениям, касающимся минимальной безопасности устройств IoT, Закон о совершенствовании кибербезопасности IoT обязывает NIST разработать - в координации с DHS, исследователями и частным сектором - руководящие принципы политики раскрытия уязвимостей для «отчетности, координации, публикации и получения» отчетов об уязвимостях в системах федерального агентства, включая устройства IoT, и системы, предлагаемые подрядчиками федеральным агентствам. Кроме того, Закон о совершенствовании кибербезопасности IoT требует пересмотра Федерального постановления о закупках, если это необходимо, и запрещает федеральным агентствам приобретать или использовать устройства IoT, если использование такого устройства может

помешать соблюдению упомянутых выше указаний по минимальной безопасности и раскрытию уязвимостей. и частный сектор - руководящие принципы политики раскрытия уязвимостей для «отчетности, координации, публикации и получения» отчетов об уязвимостях в системах федерального агентства, включая устройства IoT, и системах, предлагаемых подрядчиками федеральным агентствам. Кроме того, Закон о совершенствовании кибербезопасности IoT требует пересмотра Федерального постановления о закупках, если это необходимо, и запрещает федеральным агентствам приобретать или использовать устройства IoT, если использование такого устройства может помешать соблюдению упомянутых выше указаний по минимальной безопасности и раскрытию уязвимостей. и частный сектор - руководящие принципы политики раскрытия уязвимостей для «отчетности, координации, публикации и получения» отчетов об уязвимостях в системах федерального агентства, включая устройства IoT, и системах, предлагаемых подрядчиками федеральным агентствам. Кроме того, Закон о совершенствовании кибербезопасности IoT требует пересмотра Федерального постановления о закупках, если это необходимо, и запрещает федеральным агентствам приобретать или использовать устройства IoT, если использование такого устройства может помешать соблюдению упомянутых выше указаний по минимальной безопасности и раскрытию уязвимостей.

В соответствии с новым законом NIST должен действовать быстро. Например, он должен разработать свои стандарты и руководящие принципы безопасности к 4 марта 2021 г. Последующий обзор политики и принципов федерального агентства OMB, NIST и DHS должен быть завершен через 180 дней, а закон требует пересмотра и исправления, поскольку соответствующих руководств и сопровождающих политик и принципов каждые пять лет.

Каждое из этих положений может оказать значительное влияние на компании, ведущие бизнес или стремящиеся вести бизнес с федеральным правительством. Кроме того, эти базовые стандарты безопасности IoT будут иметь как прямое, так и косвенное каскадное воздействие на промышленность и критически важные сектора инфраструктуры. Публикации NIST регулярно становятся доктринальными стандартами, которые попадают в международное сообщество, устанавливающее стандарты, и эти стандарты неизменно принимаются частным сектором.

NIST добавляет к своему руководству по управлению рисками Интернета вещей четыре новых документа, включая руководство для федерального правительства и новый базовый документ для более широкой экосистемы Интернета вещей.

Вслед за Законом о совершенствовании кибербезопасности IoT 15 декабря 2020 года NIST выпустил четыре новых проекта документов по кибербезопасности IoT, а также обновленный каталог возможностей IoT. NIST поясняет, что новые документы «помогут решить проблемы, поднятые в [Законе], и начнут давать указания, которые предписаны законом».

Новые проекты документов содержат рекомендации для федеральных агентств и производителей устройств и «призваны помочь убедиться, что правительство и разработчики устройств IoT едины в вопросах кибербезопасности

устройств IoT, используемых федеральными агентствами». Некоторые из документов имеют более широкий охват, помимо варианта использования Интернета вещей федеральным правительством. В частности, новые проекты документов:

Проект NIST SP 800-213, Руководство по кибербезопасности устройств Интернета вещей для федерального правительства: установление требований к кибербезопасности устройств Интернета вещей.

Проект NISTIR 8259B, Базовая линия основных возможностей нетехнической поддержки IoT

Проект NISTIR 8259C, Создание профиля с использованием базовой линии IoT Core и нетехнической базы

Проект NISTIR 8259D, Profile Using the IoT Core Baseline и Нетехническая база для федерального правительства

Кроме того, NIST обновил свои каталоги требований к кибербезопасности устройств IoT в качестве дополнительного контента, который может использоваться для поддержки элементов управления NIST-800-53.

В проекте SP 800-213 содержатся инструкции для федеральных агентств по приобретению и внедрению устройств IoT. Основная суть этого документа - «руководство для федеральных агентств по определению применимых требований к кибербезопасности устройства (т. Е. Набора возможностей кибербезопасности устройства и нетехнических вспомогательных возможностей) для устройства IoT». В нем подчеркивается, что «[a] группы должны полностью понимать конкретный вариант использования устройства IoT, поскольку этот вариант использования может влиять на требования к кибербезопасности устройства», и перечисляет несколько ключевых вопросов, которые агентства должны рассмотреть.

Три новых проекта серии 8259, предназначенные для производителей устройств IoT, основаны на основных мероприятиях NIST по кибербезопасности для производителей устройств IoT и дополняют их: NISTIR 8259, Основные мероприятия по кибербезопасности для производителей устройств IoT и 8259A, Базовый уровень возможностей кибербезопасности устройств IoT. Новый проект межведомственных отчетов NIST (NISTIR) - 8259B, 8259C и 8259D - расширяет спектр рекомендаций по кибербезопасности IoT, предоставляя производителям устройств IoT дорожную карту, чтобы помочь организациям внедрить рекомендации SP 800-213:

Проект NISTIR 8259B предоставляет базовые нетехнические возможности и предназначен для дополнения базового базового уровня кибербезопасности устройств (NISTIR 8259A), который NIST уже завершил.

В проекте NISTIR 8259C подробно описан процесс разработки индивидуализированного профиля любой организацией - например, для конкретной организации или сектора промышленности - с использованием базовых технических и нетехнических возможностей NIST; и

Проект NISTIR 8259D, федеральный профиль, служит рабочим приложением NISTIR 8259C для разработки профиля для варианта использования федерального правительства.

Вместе эти документы окажут значительное влияние на экосистему Интернета вещей. NIST поясняет: «Как и в случае со всеми публикациями NIST, само руководство не является нормативным. ... Поскольку компаниям, которые ведут дела с государственными учреждениями, необходимо будет взаимодействовать с технологиями, которые правительство считает приемлемыми, руководство, вероятно, будет иметь далеко идущее влияние». (курсив мой)

Эти четыре проекта открыт для общественного обсуждения до 12 февраля 2021 года.

NIST начинает оценку механизмов доверия к безопасности Интернета вещей, в том числе этикеток и самосертификации.

Наконец, 7 января 2021 года NIST опубликовал резюме недавнего семинара по IoT, на котором основное внимание уделялось созданию федерального профиля безопасности устройств IoT. Подводя итоги, NIST сообщил, что приступит к оценке подходов к установлению уверенности в безопасности устройств IoT. В нем объясняется, что «участники семинара указали на желание большей конкретности в отношении использования оценок соответствия и других механизмов доверия, таких как маркировка и самосертификация», и отметили, что «эти механизмы доверия могут быть важным компонентом пространства решений для кибербезопасности IoT.”

Маркировка и сертификация - это непростые темы, поскольку кибербезопасность очень сложна, сложна и зависит от контекста. Кроме того, кибербезопасность - это не статичное понятие, поскольку технологии и ландшафт угроз постоянно развиваются. NIST планирует тесно сотрудничать с заинтересованными сторонами, поскольку он начинает оценивать эти подходы. Учитывая сопутствующие сложности, крайне важно, чтобы отрасль тесно взаимодействовала с NIST для достижения общих целей по установлению доверия к устройствам IoT и продолжению улучшения безопасности IoT». ***(Megan L. Brown, Sam Kaplan, Kathleen E. Scott, Boyd Garriott. 2021 Preview: How the Private Sector Will be Impacted by IoT Cybersecurity Work at NIST // Wiley Rein LLP (https://www.wiley.law/newsletter-Jan-2021-PIF-2021-Preview-How-the-Private-Sector-Will-be-Impacted-by-IoT-Cybersecurity-Work-at-NIST). 14.01.2021).***

***

«Дополнительная функция была выпущена бесплатно для пользователей в технической предварительной версии на этой неделе, добавляя новый уровень безопасности для службы, которая страдает от проблем конфиденциальности.

Производитель умных дверных звонков Ring заставляет критиков кибербезопасности меньше волноваться с введением сквозного шифрования во многие свои модели. Кольцевые продукты, которые пользовались огромным успехом у потребителей, столкнулись с целым рядом жесткой критики со стороны экспертов по кибербезопасности за то, что, по их словам, не уделялось внимания элементарной цифровой безопасности.

После долгожданного отклика на критику Ring на этой неделе внедрила сквозное шифрование для многих своих домашних камер безопасности. Сквозное

шифрование, согласно Ring, можно добавить менее чем к 50 процентам используемых продуктов. Старые модели интеллектуальных дверных звонков, такие как видеодомофоны первого и второго поколения, не могут быть обновлены с помощью дополнительной защиты.

Этот шаг был ожидаемым, но начат позже, чем планировалось.

Технические подробности компании Ring, принадлежащей Amazon, были опубликованы в среду (PDF) в рамках технического предварительного просмотра новых мер безопасности. Планы сквозного шифрования Ring были впервые объявлены в сентябре и первоначально планировалось представить к концу 2020 года.

Эта функция - которая будет необязательной и бесплатной для клиентов - позволит только устройству, авторизованному и зарегистрированному с соответствующей учетной записью Ring, принимать и получать доступ к видеопотоку Live Ring. Если третьи стороны хотят просмотреть запись или поток на другом устройстве, им потребуется доступ к ключу шифрования, хранящемуся на мобильном устройстве, авторизованном для просмотра потока.

Неясно, как это может повлиять на доступ правоохранительных органов к сигналам дверного звонка - если вообще повлияет.

Яростные критики

Компания годами подвергалась критике за недостатки в системе, которая открывала видео и данные, собранные системой, для кражи злоумышленниками. Тем не менее другие критики раскритиковали Ring за то, что, по их словам, было собственными изворотливыми методами сбора данных.

В прошлом году Amazon исправила уязвимость в интеллектуальном дверном звонке Ring, которая могла позволить злоумышленникам получить доступ к учетным данным владельца сети Wi-Fi и потенциально перенастроить устройство для запуска атаки на домашнюю сеть.

Пару дней спустя пять сенаторов США в письме к генеральному директору Amazon Джеффу Безосу потребовали, чтобы Amazon раскрыла, как она обеспечивает безопасность видеозаписей устройства домашней безопасности Ring и кому разрешен доступ к этим видеозаписям.

В октябре прошлого года Ring снова подняла критику в отношении конфиденциальности, когда представила новую камеру Always Home Cam - умную домашнюю камеру видеонаблюдения, которая летает по домам и снимает записи с камер наблюдения за людьми в их собственных домах. Из-за и без того сомнительной практики сбора данных Amazon защитники конфиденциальности обеспокоены тем, что отснятый материал может попасть в чужие руки.

Смягчение входной двери

В среду Ring рассказал, как конкретно решить эти проблемы. Компания заявила, что Ring добавит дополнительный уровень безопасности и конфиденциальности в дополнение к существующему шифрованию Ring, которое по умолчанию шифрует видео, когда они загружаются в облако и хранятся на серверах Ring.

«Благодаря сквозному шифрованию видео клиентов дополнительно защищены с помощью дополнительной блокировки, которую можно

разблокировать только с помощью ключа, который хранится на зарегистрированном мобильном устройстве клиента, разработанном таким образом, что только клиент может расшифровать и просмотреть записи на своем зарегистрированное устройство», - говорится в сообщении в блоге Ring о развертывании.

Ринг сказал, что сервис предоставляет пользователям «контроль и дополнительные возможности для шифрования и дешифрования их видео и разработан таким образом, чтобы никакая неавторизованная третья сторона не могла получить доступ к пользовательскому видеоконтенту», согласно официальному документу Ring, опубликованному в Интернете об услуге.

Видео, зашифрованные, когда функция отключена, по-прежнему будут зашифрованы, если пользователь решит отключить сквозное шифрование, согласно техническому документу, в котором также содержатся пошаговые инструкции о том, как работает функция, а также конкретные сведения о какой тип шифрования использует компания.

Сквозное шифрование, безусловно, добавляет уровень конфиденциальности, который многие клиенты и защитники конфиденциальности давно хотели получить от Ring, которое с момента своего создания постоянно раздвигало границы того, насколько конфиденциально люди готовы отказаться от защиты домашней безопасности.

Следуя примеру Zoom

Этот шаг, чтобы добавить конец в конец шифрования Ring похож на тот, который онлайн - сервис видеоконференцсвязи Увеличить принял в прошлом году, чтобы зашифровать видеопотоков на фоне опасений о конфиденциальности и многочисленных нарушений безопасности службы, такие как зум бомбардировочных и нулевого дня уязвимости, среди другие. Однако Zoom сделал эту функцию доступной только для платных пользователей сервиса.

Хотя новая функция Ring имеет преимущества в отношении конфиденциальности и безопасности, она также нарушит некоторые существующие функции службы, такие как доступ к видео Ring через Alexa, а также устройство Echo Show или Fire TV или совместное использование с другими камерами.

Шифрование также может помешать спорным планам использования приложения Ring's Neighbours для обмена кадрами данных с устройств Ring с правоохранительными органами, например, что происходит в программе, проверяемой полицией в Миссисипи, в которой они могут транслировать видео с камер Ring, установленных в частные дома и предприятия. После запуска программа стала тревожным звонком для защитников конфиденциальности, таких как Electronic Frontier Foundation, которые назвали запуск программы своими «худшими опасениями» «подтвержденными».

Однако, поскольку эта функция является необязательной, и пользователи Ring могут выбрать передачу ключей шифрования третьим лицам, по-прежнему будет возможно передавать потоковое видео на другие устройства и обмениваться видеопотоками с правоохранительными органами, если владелец устройства решит». ***(Elizabeth Montalbano. Ring Adds End-to-End Encryption to Quell Security***

Uproar // Threatpost (https://threatpost.com/ring-adds-end-to-end-encryption-to-quell-security-uproar/163042/). 14.01.2021).

***

«Велотренажер Peloton президента США Джо Байдена викликає підозри і питання у Секретної служби і охорони Білого дому…

Велотренажер може нести ризик кібербезпеці.

Велотренажер марки Peloton, яким користується Джо Байден, оснащений вбудованою камерою і мікрофоном, підключений до мережі інтернет. Саме тренажер став камені спотикання під час підготовки переїзду Байденом в Білий дім.

Тренажер Peloton, вартістю більш 2,5 тисячі доларів, поєднує в собі тренажер і планшет з доступом в інтернет, що дозволяє під час тренування вести трансляції, відвідувати онлайн-заняття і таке інше. Крім того, між пристроями створена мережа, в якій гонщики можуть змагатися на основі показників тренувань.

Цей велотренажер став незамінним інструментом для тренувань Байдена в період карантину, пов'язаного з пандемією.

Тим не менш, як пише NYT, експерти з кібербезпеки впевнені - Байден не залишиться без свого велотренажера, адже Секретна служба напевно може його убезпечити, хоча після цього його програмне забезпечення буде вже не зовсім таким, як раньше. Видання повідомляє, що Байден не перший президент, щу поставив питання про особисту кібербезпеку. До нього Секретній службі доводилося врегулювати ситуацію з Дональдом Трампом, який хотів дзвонити з особистого iPhone і Бараком Обамою, який привіз в Білий дім телефон BlackBerry, а пізніше захотів використовувати iPad, що також не відповідало поняттям про кібербезпеку в Білому домі.

Нагадаємо, Джо Байден 20 січня офіційно вступив на посаду президента США». ***(Тетяна Юдіна. Велотренажер Байдена викликає питання у охорони Білого дому: і ось чому // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1913417-velotrenazher-baydena-viklikaye-pitannya-u-okhoroni-bilogo-domu-i-os-chomu). 21.01.2021).***

***

Кіберзлочинність та кібертерроризм

«Исследователи предупреждают, что в ближайшие месяцы сектор здравоохранения должен подготовиться к росту числа кибератак и различных векторов атак.

Во вторник компания Check Point, занимающаяся кибербезопасностью, опубликовала новые статистические данные, которые показывают, что с ноября кибератаки на мировой сектор здравоохранения увеличились на 45%, что более чем вдвое превышает рост на 22% по сравнению со всеми отраслями промышленности мира за тот же период.

По мнению исследователей, векторы атак, используемые злоумышленниками, разнообразны; включая распределенные атаки типа «отказ в

обслуживании» (DDoS), социальную инженерию, ботнеты, фишинг и программы-вымогатели.

Однако серьезную озабоченность вызывает, в частности, программа-вымогатель.

Мы уже видели, насколько изнурительной может быть волна атак программ-вымогателей. WannaCry вспышка 2017 года заперта и разрушала операции для бесчисленных предприятий по всему миру, и в течение последних четырех лет, вымогатели продолжает расти в популярности из - за того, как прибыльным преступником бизнеса стало.

Когда дело доходит до больниц, некоторые провайдеры будут платить шантаж, требуемый операторами программ-вымогателей, вместо того, чтобы рисковать лечением пациентов. Смерть пациента в результате атаки программы-вымогателя на больницу уже произошла.

Check Point сообщает, что количество атак программ-вымогателей в секторе здравоохранения растет. Штамм-вымогатель Ryuk в настоящее время является самым популярным вредоносным ПО для этих атак, за ним следует Sodinokibi.

Всего в ноябре на медицинские учреждения еженедельно регистрировалось 626 атак по сравнению с 430 в октябре. За последние два месяца больше всего пострадала Центральная Европа, где на 145% увеличилось количество атак, связанных со здравоохранением, за ней следуют Восточная Азия, Латинская Америка, а затем остальные страны Европы и Северная Америка.

Медицинские организации в Канаде и Германии испытали самый большой рост числа кибератак - 250% и 220% соответственно.

Check Point заявляет, что причина увеличения - финансовая, поскольку злоумышленники стремятся нажиться на всемирных сбоях, вызванных COVID-19. В то время как стандартные мошенники нацелены на широкую публику с помощью фишинга, электронной почты, текстовых сообщений и телефонных звонков в кампаниях, связанных с коронавирусом, другие группы надеются получить прибыль за счет более изнурительных атак на основные службы.

«Поскольку внимание мира по-прежнему сосредоточено на борьбе с пандемией, киберпреступники также будут продолжать использовать и пытаться использовать этот фокус в своих собственных незаконных целях, поэтому важно, чтобы как организации, так и отдельные лица поддерживали хорошую кибергигиену, чтобы защитить себя от Интернет-преступление, связанное с covid, - говорит команда». ***(Charlie Osborne. As coronavirus cases surge, so do cyberattacks against the healthcare sector // ZDNet (https://www.zdnet.com/article/as-coronavirus-cases-surge-so-do-cyberattacks-against-the-healthcare-sector/). 05.01.2021).***

***

«Правительство Австралии предупреждает о продолжающейся кампании, выдающихся себя за Австралийский центр кибербезопасности (ACSC), для заражения целей вредоносным ПО.

Мошенники, координирующие эти атаки, также активно пытаются убедить потенциальных жертв установить программное обеспечение для удаленного

администрирования и совместного использования рабочего стола с конечной целью кражи банковской информации.

«Австралийский центр кибербезопасности (ACSC) предупреждает, что некоторые австралийцы получают телефонные звонки или электронные письма от мошенников, утверждающих, что они являются сотрудниками ACSC, и что компьютер получателя был взломан», - предупредило агентство по кибербезопасности.

Электронные письма, отправленные этими злоумышленниками, маскируются под официальные сообщения, доставленные ACSC, которые пытаются убедить австралийцев на принимающей стороне загрузить антивирусное программное обеспечение по вредоносным ссылкам.

Как только они загрузят его и запустят на своих компьютерах, жертвы заразятся неизвестным вредоносным программным обеспечением, которое потенциально может позволить мошенникам захватить их компьютеры и украсть конфиденциальную информацию.

Сообщения о мошеннических телефонных звонках, направленных на банковскую информацию

«Помимо электронных писем, были сообщения о киберпреступниках, которые звонили людям с поддельного австралийского номера телефона с просьбой загрузить TeamViewer или AnyDesk на свое устройство, чтобы помочь решить проблемы с вредоносным ПО», - добавили в ACSC.

«Затем мошенник пытается убедить получателей принять меры, например, ввести URL-адрес в браузере и получить доступ к онлайн-банковским сервисам, которые затем взламывают их компьютер, чтобы раскрыть банковскую информацию».

Австралийцам, которые стали жертвами этой кампании или которые хотят узнать больше об этих продолжающихся атаках, рекомендуется связаться с ACSC по телефону 1300 292 371 (1300 CYBER 1).

В прошлом году ACSC также предупредил о телефонных мошенниках, выдающих себя за государственные учреждения и предприятия Австралии.

В рамках этих атак мошенники пытались убедить своих жертв передать учетные данные, которые они впоследствии могли использовать для установки приложений удаленного доступа для входа в банковские и онлайн-счета жертв для кражи финансовой информации…». ***(Sergiu Gatlan. Australian cybersecurity agency used as cover in malware campaign // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/australian-cybersecurity-agency-used-as-cover-in-malware-campaign/). 05.01.2021).***

***

«По мере того как учащиеся, семьи и округа переходили от традиционных моделей обучения к дистанционному обучению, эксперты внутри и вне правительства начали прогнозировать и видеть всплеск кибератак, направленных на школьные сети. Во вторник, 24 ноября 2020 года, государственная школьная система округа Балтимор стала последней - хотя, конечно, не единственной - школьной системой, которой препятствует то, что

школьные чиновники назвали «катастрофической атакой на нашу технологическую систему».

Хотя подробностей на данный момент мало, атака разыгралась, как и многие предыдущие. Одна за другой районные системы начали медленно отключаться. Прервана прямая видеотрансляция заседания школьного совета, учителя заметили проблемы с системой выставления оценок округа, а веб-сайт округа, приложения электронной почты и платформа дистанционного обучения были закрыты. Атака была настолько обширной, что школы были закрыты на несколько дней, пока район не осознавал размах инцидента.

Судя по публикациям в социальных сетях, зашифрованные файлы имеют расширение, связанное с семейством программ-вымогателей, впервые появившихся в 2018 году. Программы- вымогатели, для тех, кто не знаком, - это категория вредоносных программ, которые блокируют файлы или целые системы до получения выкупа оплачивается. Особенно коварная особенность программы-вымогателя, которая, возможно, обнаружена в атаке на Балтимор, - это функция, которая позволяет злоумышленникам отключить функцию восстановления системы Windows, что еще больше затрудняет восстановление. К счастью, руководство школы «не верят, что личные данные учащихся или сотрудников были украдены» во время атаки. Тем не менее, как это часто бывает, округ покрывает расходы на кредитный мониторинг «для всех учащихся и сотрудников школ округа».

Для тех, кто задается вопросом, избавиться от болтов, связанных с атакой программ-вымогателей, нелегко и непросто. В дополнение к тому факту, что платежи обычно требуются в криптовалюте, и требования неуклонно росли, Управление по контролю за иностранными активами Министерства финансов США недавно предупредило, что оплата требований программ-вымогателей может нарушить федеральный закон. Фактически, «OFAC может налагать гражданско-правовые санкции за нарушение санкций на основе строгой ответственности, что означает, что лицо, подпадающее под юрисдикцию США, может быть привлечено к гражданской ответственности, даже если оно не знало или не имело оснований знать, что оно участвует в сделке с лицом. это запрещено законами и постановлениями о санкциях, администрируемыми OFAC».

Почему школьные округа? Проще говоря, они - привлекательная цель. Данные ребенка очень ценны, так как у него часто не будет большой кредитной истории, если она вообще есть, и они могут не осознавать, что их номер социального страхования был скомпрометирован, пока они не попытаются получить кредит много лет спустя. Кроме того, у школ может не быть ресурсов для надлежащей защиты своих сетей или обновления оборудования. Поскольку большая часть обучения проводится удаленно, эти уязвимости только увеличиваются…». ***(Jeff Knight. Cyberattacks aimed at school networks // Bricker & Eckler LLP. (https://www.bricker.com/insights-resources/publications/cyberattacks-aimed-at-school-networks). 08.01.2021).***

***

«Фишинговые рассылки на тему пандемии COVID-19, атаки на системы дистанционного обучения и кибершпионаж будут в трендах кибератак 2021 года, заявил глава представительства Check Point Software Technologies Василий Дягилев.

По его словам, COVID-19 не скоро покинет заголовки статей, новости о разработке вакцины и введении новых ограничений продолжат использоваться в фишинговых атаках, как и в 2020 году.

Фармацевтические компании, занимающиеся разработкой вакцины, снова будут подвергаться кибератакам мошенников или хакеров, заинтересованных в эскалации проблемы, ожидает он.

Другим трендом будут атаки на системы дистанционного обучения, в том числе со стороны школьников. В августе число подобных кибератак, в том числе и от хакеров-тинейджеров, за неделю выросло на 30%. «Школьные хулиганы» продолжат атаковать системы дистанционного обучения, прогнозирует Дягилев.

Также в 2021 году, по его мнению, стоит ожидать и кибератак с целью шпионажа. Так, устройства, помогающие следить за здоровьем, будут собирать данные о самочувствии пользователей, «подключенные автомобили» — следить за передвижениями, а системы «умного» города — накапливать информацию о нашей жизни.

Также по мере развертывания сетей 5G в мире количество подключенных устройств Интернета вещей увеличится, что сделает сети более уязвимыми к масштабным мультивекторным кибератакам.

«Умные» устройства, подключенные к сетям и облакам, по-прежнему являются слабым звеном с точки зрения информационной безопасности: с одной стороны, они не дают полного доступа к своим данным, с другой стороны, имеют особые требования к безопасности, отметил Дягилев». ***(Эксперт назвал тренды кибератак 2021 года // Finance.ua (https://news.finance.ua/ru/news/-/484846/ekspert-nazval-trendy-kiberatak-2021-goda). 06.01.2021).***

***

«Почти половина всех фишинговых атак, направленных на кражу учетных данных, таких как адреса электронной почты и пароли, путем имитации известных брендов, выдает себя за Microsoft.

Исследователи кибербезопасности в Check Point проанализировали фишинговые письма, отправленные за последние три месяца, и обнаружили, что 43% всех попыток фишинга, имитирующих бренды, пытались выдать себя за сообщения от Microsoft.

Microsoft - популярная приманка из-за широкого распространения Office 365 среди предприятий. Похищая эти учетные данные, преступники надеются получить доступ к корпоративным сетям.

А поскольку в течение последнего года многие организации переходят на удаленную работу, чтобы обеспечить социальное дистанцирование, электронная почта и обмен сообщениями в Интернете стали еще более важными для бизнеса - и это то, чем кибератаки активно пытаются использовать.

Сотрудники не только полагаются на электронную почту для повседневного общения со своими товарищами по команде и начальниками, они также не всегда имеют одинаковую осведомленность о безопасности и защиту при работе из дома.

В случае этих атак, даже если сообщения не предназначены для того, чтобы выглядеть так, как будто они исходят от самой Microsoft, и они могут утверждать, что исходят от коллеги, отдела кадров, поставщика или кого-либо еще, с кем человек может вступить в контакт, фишинг-ссылки или Приложение попросит пользователя ввести свои данные для входа, чтобы «подтвердить» свою личность.

Если адрес электронной почты и пароль вводятся на этих страницах, которые выглядят как сайт входа в Microsoft, злоумышленники могут их украсть. Украденные учетные данные могут быть использованы для получения дополнительного доступа к взломанной сети или могут быть проданы другим киберпреступникам на торговых площадках дарквеба.

Вторым наиболее часто имитируемым брендом в период анализа была DHL: на атаки, имитирующие поставщика логистических услуг, приходилось 18% всех попыток фишинга бренда. DHL стала популярной фишинг-приманкой для преступников, потому что многие люди теперь застревают дома из-за ограничений COVID-19 и получают больше доставок, поэтому люди с большей вероятностью ослабят бдительность, когда увидят сообщения, якобы отправленные от фирмы доставки.

В фишинговых письмах часто фигурируют и другие бренды, включая LinkedIn, Amazon, Google, PayPal и Yahoo. Взлом любой из этих учетных записей может предоставить киберпреступникам доступ к конфиденциальной личной информации, которую они могут использовать.

«В четвертом квартале 2020 года преступники активизировали свои попытки украсть личные данные людей, выдавая себя за ведущие бренды, и наши данные ясно показывают, как они меняют свою фишинговую тактику, чтобы увеличить свои шансы на успех», - сказала Майя Горовиц, директор по анализу угроз и исследованиям в Check Точка.

"Как всегда, мы призываем пользователей проявлять осторожность при разглашении личных данных и учетных данных бизнес-приложениям и дважды подумать, прежде чем открывать вложения или ссылки в сообщениях электронной почты, особенно в сообщениях электронной почты, которые, как утверждается, от компаний, таких как Microsoft или Google, которые с наибольшей вероятностью выдавать себя за другое лицо ", - добавила она.

Также можно обеспечить дополнительный уровень защиты для Microsoft Office 365 и других корпоративных учетных записей, применив двухфакторную аутентификацию, так что даже если киберпреступникам удастся украсть имя пользователя и пароль, дополнительный уровень проверки, необходимый для двухфакторной аутентификации поможет сохранить учетную запись в безопасности». ***(Danny Palmer. Phishing warning: These are the brands most likely to be impersonated by crooks, so stay alert // ZDNet (https://www.zdnet.com/article/phishing-warning-these-are-the-brands-most-likely-to-be-impersonated-by-crooks-so-stay-alert/). 14.01.2021).***

***

«Команды кибербезопасности сталкиваются с новыми проблемами в том, как они работают, поскольку пандемия Covid-19 вынудила многие операционные центры безопасности (SOC) работать удаленно, а также иметь дело с новыми угрозами - все это приводит к увеличению рабочих нагрузок и увеличению усталости персонала.

Исследование, проведенное институтом Ponemon и Respond Software, в ходе опроса сотрудников службы информационной безопасности показало, что пандемия коронавируса увеличивает часы и нагрузку на сотрудников в профессии, которая уже была средой высокой интенсивности для людей.

События 2020 года привели к тому, что многие офисные команды перешли к удаленной работе, и это было то же самое для значительного числа специалистов по кибербезопасности. В результате пандемии более одной трети сред SOC перешли на удаленную работу. Понятно, что это произошло для защиты людей от вируса, но более половины тех, кто сейчас работает удаленно, говорят, что это повлияло на работу.

Это происходит в то время, когда командам безопасности приходится иметь дело с целым рядом угроз, включая фишинг, вредоносное ПО и программы-вымогатели, а защита от них становится еще более сложной задачей, поскольку компании адаптировались к целой рабочей силе, работающей из дома.

Переход к удаленной работе предоставил киберпреступникам и хакерам-злоумышленникам дополнительные возможности для потенциально проникновения в корпоративные сети, когда сотрудники подключаются к рабочим системам через домашние интернет-соединения и даже со своих персональных компьютеров.

Это создало дополнительные проблемы для обеспечения безопасности конечных точек, когда это уже было сложно в корпоративной среде - в то время как службы безопасности также пытаются сбалансировать работу с дополнительным давлением работы из дома.

«Удаленная работа требует отвлекающих факторов, которых обычно не бывает в физическом SOC, таких как семья, друзья, домашние животные, соседи по комнате или даже отсутствие хорошей домашней обстановки, например, работа с дивана по сравнению с обычным столом», - Крис Триоло - сообщил ZDNet вице-президент Respond Software.

«Из-за этого аналитику может быть трудно оставаться продуктивным и сосредоточиться на защите от злоумышленников, как им следует, создавая дополнительный стресс для аналитика SOC».

Согласно опросу, дополнительное давление, связанное с работой в сфере кибербезопасности, одновременно с работой из дома, снизило моральный дух сотрудников SOC, причем три четверти заявили, что в результате они испытали выгорание.

Степень выгорания настолько велика, что некоторые аналитики по безопасности оставляют свои должности, в то время как организации пытаются привлечь и удержать сотрудников, предлагая более высокие зарплаты, чем когда-

либо прежде. Согласно исследованию, средняя зарплата аналитика по безопасности составляет 111 000 долларов по сравнению со 102 000 долларов годом ранее.

"SOC работает лучше всего, когда он работает лично, и большинство профессионалов отрасли, вероятно, согласятся с этим мнением. Однако можно с уверенностью сказать, что некоторые организации могут предпочесть держать SOC удаленно из-за различных факторов, включая снижение стоимости аренды офисных помещений., - сказал Триоло.

Что бы ни случилось, организациям необходимо научиться управлять кибербезопасностью, когда сотрудники не могут работать из офиса, и быть более подготовленными, если другое событие заставит аналогичную схему удаленной работы в будущем.

«Независимо от того, вернется ли SOC к тому, чтобы стать личным лицом, организации теперь узнали, что планы действий в случае стихийных бедствий и чрезвычайных ситуаций должны выходить за рамки простого физического бедствия, такого как пожар или наводнение. Мы должны начать думать о таких ситуациях, как пандемия, при которой аналитики безопасности могут быть физически перемещены и не могут безопасно находиться в одной комнате вместе на работе», - сказал Триоло». ***(Danny Palmer. Cybersecurity teams are struggling with burnout, but the attacks keep coming // ZDNet (https://www.zdnet.com/article/cybersecurity-teams-are-struggling-with-burnout-but-the-attacks-keep-coming/). 12.01.2021).***

***

«Злоумышленники взламывают проверенные учетные записи в Твиттере в рамках аферы Илона Маска с раздачей криптовалюты, которая в последнее время стала широко активной.

Нет ничего нового в мошенничестве с криптовалютой в Твиттере, особенно в том, что притворяется раздачей от Илона Маска. В 2018 году мошенники заработали 180000 долларов, используя успешную аферу Илона Маска с раздачей подарков, продвигаемую в Twitter.

За последнюю неделю исследователь безопасности MalwareHunterTeam заметил рост числа проверенных аккаунтов в Твиттере, взломанных в результате мошенничества, продвигающего очередную поддельную раздачу криптовалюты Илона Маска.

Эти учетные записи будут отвечать на твиты, подобные приведенным ниже твитам Илона Маска, и продвигать мошенничество, в котором Маск якобы раздает бесплатную криптовалюту.

Твиты будут содержать ссылки, которые перенаправляют на статью Medium, рекламирующую поддельную раздачу. Статьи содержат дополнительные ссылки на целевые страницы мошенничества, в которых указано, что если вы отправите биткойны на указанный адрес, они отправят вам обратно вдвое большую сумму.

Хотя большинство этих твитов используют в качестве темы Илона Маска, некоторые из взломанных учетных записей также продвигают поддельные подарки от Тайлера Винклвосса из Gemini Exchange.

Команда MalwareHunterTeam сообщила BleepingComputer, что большинство учетных записей, взломанных с помощью этого мошенничества, бездействовали без действий со стороны владельца.

«Большой %, но не все. По крайней мере, 2-3 были активны в течение от нескольких недель до нескольких дней, из них казалось возможным, что последние действия были не от первоначального владельца, но, конечно, не удалось проверить», - пояснила команда MalwareHunterTeam.

Поскольку Twitter отключил возможность проверки учетной записи в июле после того, как компания была взломана в результате масштабного мошенничества с криптовалютой, проверенные учетные записи пользуются большим спросом у злоумышленников.

Злоумышленники, скорее всего, нацелены на бездействующие проверенные учетные записи, которые не будут обнаружены владельцем учетных записей…

Мошенники зарабатывают более 580 тысяч долларов за неделю

Эта афера оказалась очень успешной для злоумышленников.

По адресам криптовалюты, собранным с целевых страниц, просмотренных BleepingComputer и MetaMask, злоумышленники заработали 587000 долларов в биткойнах…

Мошенничество с раздачей Ethereum не принесло результатов, а мошенникам было принесено всего 2700 долларов…

Поскольку с этим мошенничеством связано много целевых страниц, возможно, что некоторые из них более успешно выманивали у людей их активы.

Важно понимать, что Илон Маск, Тесла, Близнецы Винклвосс не будут отправлять вам криптовалюту и что все эти раздачи являются мошенничеством…». ***(Lawrence Abrams. Verified Twitter accounts hacked in $580k 'Elon Musk' crypto scam // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/verified-twitter-accounts-hacked-in-580k-elon-musk-crypto-scam/). 14.01.2021).***

***

«Project Zero, команда Google по поиску ошибок 0day, раскрыла хакерскую кампанию, координируемую «очень искушенным актером» и нацеленную на пользователей Windows и Android с помощью эксплойтов нулевого и n-го дня.

Команда Project Zero в сотрудничестве с Google Threat Analysis Group (TAG) в начале 2020 года обнаружила атаку водопоя с использованием двух серверов эксплойтов, каждый из которых использует отдельные цепочки эксплойтов для компрометации потенциальных целей.

«Эти цепочки эксплойтов разработаны для обеспечения эффективности и гибкости благодаря своей модульности», - сказал Project Zero после их анализа в течение нескольких месяцев.

«Это хорошо спроектированный, сложный код с множеством новых методов эксплуатации, зрелым журналированием, сложными и рассчитанными методами постэксплуатации, а также большим объемом антианалитических и целевых

проверок. Мы считаем, что группы экспертов спроектировали и разработали их эксплуатировать цепочки».

Исследователи Project Zero смогли собрать массу информации с двух серверов эксплойтов, в том числе:

Рендерер использует четыре ошибки в Chrome, одна из которых на момент обнаружения все еще была нулевой.

Два эксплойта для выхода из песочницы, использующие три уязвимости нулевого дня в Windows.

«Набор для повышения привилегий», состоящий из широко известных эксплойтов n-day для старых версий Android.

Один из серверов эксплойтов, использованных в этой операции взлома, использовался для нацеливания на пользователей Windows, а другой специально пытался взломать устройства Android.

В обоих случаях злоумышленники использовали эксплойты Chrome для удаленного выполнения вредоносного кода на целевых устройствах, удаленного выполнения кода, нулевого дня для устройств Windows и n-дня для Android.

Хотя в цепочке эксплойтов Android не использовались Android-дни нулевого дня, "[b] учитывая изощренность актера, мы думаем, что вполне вероятно, что у них был доступ к Android 0-days, но мы не обнаружили ничего в нашем анализе", - сказал Project Zero…

«Помимо эксплуатации, их выделяют модульность полезной нагрузки, взаимозаменяемые цепочки эксплуатации, ведение журнала, нацеливание и зрелость операций этого актора», - добавил Project Zero.

«Мы надеемся, что, публикуя эту информацию публично, мы продолжаем сокращать разрыв в знаниях между частной эксплуатацией (что хорошо финансируемые группы по эксплуатации делают в реальном мире) и тем, что общеизвестно».

Четыре нулевых дня, использованные в этих атаках и исправленные в прошлом году:

CVE-2020-6418 - уязвимость Chrome в TurboFan (исправлено в феврале 2020 г.)

CVE-2020-0938 - уязвимость шрифтов в Windows (исправлено в апреле 2020 г.)

CVE-2020-1020 - уязвимость шрифтов в Windows (исправлено в апреле 2020 г.)

CVE-2020-1027 - уязвимость Windows CSRSS (исправлено в апреле 2020 г.)

Все три нулевых дня Windows были рассмотрены Microsoft во вторник патчей в апреле 2020 года, а нулевой день Chrome был исправлен Google в феврале 2020 года с выпуском Chrome 80.0.3987.122 после обнаружения уязвимости в дикой природе.

Команда Project Zero также опубликовала отдельные отчеты о Chrome "Infinity Bug", используемом для нацеливания на пользователей Android, цепочках эксплойтов Chrome, Android и Windows, а также о процедуре постэксплуатации, используемой на рутированных и скомпрометированных устройствах Android, как показано в атаки». ***(Sergiu Gatlan. Google discloses hacking campaign targeting***

Windows, Android users // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/google-discloses-hacking-campaign-targeting-windows-android-users/). 13.01.2021).

***

«Киберпреступники часто используют атаки методом перебора, фишинговые электронные письма и существующие дампы данных для проникновения в корпоративные сети, но есть одна область, которая часто игнорируется в ущерб компании: учетные записи-призраки.

Не всегда бывает так, что когда сотрудник увольняется с работы, будь то из-за нового предложения о работе, изменения обстоятельств, болезни или, в неблагоприятных случаях, смерти, его учетные записи удаляются из корпоративных сетей.

Этим недосмотром киберпреступники сейчас пользуются, а в недавнем случае активно использовали для распространения программ-вымогателей.

В тематическом исследовании, задокументированном кибер-криминалистической группой Rapid Response компании Sophos во вторник, организация обратилась за помощью после заражения вымогателем Nemty.

Согласно Sophos, программа-вымогатель, также известная как Nefilim, затронула более 100 систем, зашифровав ценные файлы и потребовав оплаты в обмен на ключ дешифрования.

Nemty, впервые обнаруженный в 2019 году, представлял собой разновидность вредоносного ПО типа Ransomware-as-a-Service (RaaS), которое можно было купить на подпольных форумах. В 2020 году разработчики взяли Nemty частный, оставляя за собой разработку Кодекса будущего для избранных партнеров.

Во время расследования источника заражения Sophos сузил первоначальное сетевое вторжение до учетной записи администратора высокого уровня. В течение месяца злоумышленники незаметно исследовали ресурсы компании, получая учетные данные администратора домена и удаляя сотни гигабайт данных.

После того, как кибератаки завершили разведку и забрали все ценное, Немти был развернут.

«Программы-вымогатели - это последняя полезная нагрузка в более длительной атаке», - отметил Питер Маккензи, менеджер Rapid Response. «Это злоумышленник сообщает вам, что он уже контролирует вашу сеть и завершил основную часть атаки. Выявить, что вы подверглись атаке программы-вымогателя, несложно, важно установить, что злоумышленник был в вашей сети неделей ранее».

Команда кибербезопасности спросила, кому принадлежит учетная запись администратора с высокими привилегиями. Компания-жертва заявила, что учетная запись принадлежала бывшему сотруднику, который скончался примерно за три месяца до кибериントрузии.

Вместо того, чтобы отозвать доступ и закрыть «призрачную» учетную запись, фирма решила оставить ее активной и открытой, «потому что были услуги, для которых она использовалась».

Sophos предлагает, чтобы для любой учетной записи-призрака, которой разрешено оставаться подключенной к корпоративным ресурсам, когда пользователю она не нужна, следует отключить интерактивный вход или, если учетная запись действительно необходима, вместо нее следует создать учетную запись службы.

Кроме того, команда утверждает, что меры нулевого доверия должны быть реализованы в масштабах всей компании, чтобы уменьшить потенциальные поверхности для атак.

В другом случае, отмеченном Sophos, новая учетная запись пользователя была тайно создана в корпоративной сети и добавлена в группу администраторов домена в Active Directory, и эта учетная запись использовалась для удаления примерно 150 виртуальных серверов и развертывания Microsoft BitLocker для шифрования существующих резервных копий серверов. нагромождение давления для оплаты». ***(Charlie Osborne. Cybercriminals use deceased staff accounts to spread Nemty ransomware // ZDNet (https://www.zdnet.com/article/cybercriminals-use-deceased-staff-accounts-to-spread-nemty-ransomware/). 26.01.2021).***

***

«Производитель сетевых устройств SonicWall заявил в пятницу вечером, что расследует нарушение безопасности своей внутренней сети после обнаружения того, что он назвал «скоординированной атакой».

В коротком заявлении, опубликованном на портале ее базы знаний, компания заявила, что «очень изощренные злоумышленники» нацелились на ее внутренние системы, «используя вероятные уязвимости нулевого дня в некоторых продуктах безопасного удаленного доступа SonicWall».

Компания изначально указала, что клиенты NetExtender VPN и шлюзы Secure Mobile Access (SMA) подверглись воздействию, но в обновлении, опубликованном несколько часов спустя, сообщила, что только устройства, входящие в ее серию SMA 100, все еще находятся в стадии расследования как содержащие уязвимость нулевого дня.

Патчи для уязвимостей нулевого дня недоступны на момент написания.

Чтобы обеспечить безопасность сетей своих клиентов, поставщик включил в свою статью базы знаний ряд мер по снижению рисков, таких как развертывание брандмауэра для ограничения взаимодействия с устройствами SMA или отключение доступа через VPN-клиент NetExtender к своим брандмауэрам.

SonicWall также призвала компании включить в своих продуктах двухфакторную аутентификацию для учетных записей администраторов.

Производитель сетевых устройств, продукты которого часто используются для защиты доступа к корпоративным сетям, теперь становится четвертым поставщиком средств безопасности, обнаружившим нарушение безопасности за последние два месяца после FireEye, Microsoft и Malwarebytes.

Все три предыдущие компании были взломаны во время атаки на цепочку поставок SolarWinds. CrowdStrike заявила, что она также была целью взлома SolarWinds, но атака не увенчалась успехом…». ***(Catalin Cimpanu. SonicWall says it was hacked using zero-days in its own products // ZDNet***

(https://www.zdnet.com/article/sonicwall-says-it-was-hacked-using-zero-days-in-its-own-products/). 23.01.2021).

***

«Хакеры, стоящие за атакой программ- вымогателей на Шотландское агентство по охране окружающей среды (SEPA), опубликовали тысячи украденных файлов после того, как организация отказалась выплатить выкуп.

В канун Рождества государственный регулирующий орган Шотландии по защите окружающей среды подвергся атаке с использованием программ-вымогателей, в ходе которой киберпреступники украли 1,2 ГБ данных. Спустя почти месяц после атаки сервисы SEPA по-прежнему не работают, но, несмотря на это, агентство дало понять, что не будет взаимодействовать с теми, кто стоит за атакой.

SEPA не подтвердила, жертвой какой формы вымогателя она стала, но ответственность за атаку взяла на себя банда вымогателей Conti.

В результате неплатежа Conti опубликовала все украденные данные на своем веб-сайте, разместив более 4000 документов и баз данных, связанных с контрактами, коммерческими услугами и стратегией. Последнее обновление от SEPA подтверждает, что по крайней мере 4000 файлов были украдены и опубликованы.

«Нам было ясно, что мы не будем использовать государственные финансы для оплаты серьезных и организованных преступников, намеревающихся нарушить работу государственных служб и вымогать государственные средства», - сказал Терри А'Хирн, исполнительный директор SEPA.

«Мы выполнили наши юридические обязательства и обязанность проявлять осторожность в отношении конфиденциальной обработки данных и, следуя совету полиции Шотландии, подтверждаем, что украденные данные были незаконно опубликованы в Интернете. Мы быстро работаем с межведомственными партнерами для восстановления и проанализировать данные, а затем, по мере подтверждения идентификации, связаться с затронутыми организациями и отдельными лицами и оказать им поддержку», - добавил он.

Агентства, с которыми SEPA работает в постоянных усилиях по расследованию атаки и полному восстановлению сети, включают правительство Шотландии, полицию Шотландии и Национальный центр кибербезопасности (NCSC).

Несмотря на последствия атаки, SEPA по-прежнему может предоставлять услуги по прогнозированию и предупреждению наводнений, а также услуги по регулированию и мониторингу…». ***(Danny Palmer. Hackers publish thousands of files after government agency refuses to pay ransom // ZDNet (https://www.zdnet.com/article/hackers-publish-thousands-of-files-after-government-agency-refuses-to-pay-ransom/). 22.01.2021).***

***

«Киберпреступная банда может усилить нежелательный трафик в рамках DDoS атак Windows Remote Desktop Protocol (RDP), - предупреждает охранная фирма NetScout и советует быть в боевой готовности во вторник.

Не все серверы RDP могут подвергаться злоупотреблениям, а только системы, в которых аутентификация RDP также включена на UDP-порт 3389 поверх стандартного TCP-порта 3389.

Netscout заявила, что злоумышленники могут отправлять искаженные UDP-пакеты на UDP-порты серверов RDP, которые будут отражены в цель DDoS-атаки, увеличившись в размере, что приведет к попаданию нежелательного трафика в систему цели.

Это то, что исследователи безопасности называют фактором усиления DDoS, и он позволяет злоумышленникам, имеющим доступ к ограниченным ресурсам, запускать крупномасштабные DDoS-атаки путем усиления нежелательного трафика с помощью систем, открытых в Интернете.

В случае RDP, Netscout заявила, что коэффициент усиления составляет 85,9, при этом злоумышленники отправляют несколько байтов и генерируют «пакеты атаки», которые «имеют длину последовательно 1260 байтов».

Фактор 85,9 ставит RDP в верхний эшелон векторов усиления DDoS, с такими как серверы Jenkins (~ 100), DNS (до 179), WS-Discovery (300-500), NTP (~ 550) и Memcached (~ 50 000).

СЕРВЕРЫ RDP УЖЕ ИСПОЛЬЗУЮТСЯ ДЛЯ РЕАЛЬНЫХ АТАК

Но плохие новости не заканчиваются на коэффициенте усиления. Netscout сообщила, что злоумышленники также узнали об этом новом векторе, которым сейчас активно злоупотребляют.

«Как это обычно бывает с новыми векторами DDoS-атак, похоже, что после начального периода использования продвинутыми злоумышленниками с доступом к индивидуализированной инфраструктуре DDoS-атак отражение / усиление RDP было превращено в оружие и добавлено в арсеналы так называемых загрузочных / stresser DDoS-наемные услуги, делая их доступными для большинства злоумышленников», - говорят исследователи.

Теперь Netscout просит системных администраторов, которые запускают серверы RDP, доступные в Интернете, перевести системы в автономный режим, переключить их на эквивалентный порт TCP или разместить серверы RDP за VPN, чтобы ограничить круг лиц, которые могут взаимодействовать с уязвимыми системами.

В настоящее время Netscout заявила, что обнаруживает более 33000 серверов RDP, открытых онлайн и работающих на UDP-порте 3389…». ***(Catalin Cimpanu. Windows RDP servers are being abused to amplify DDoS attacks // ZDNet (https://www.zdnet.com/article/windows-rdp-servers-are-being-abused-to-amplify-ddos-attacks/). 22.01.2021).***

***

«Как сообщает The Register, партия ноутбуков, поставленных в британские школы Министерством образования для помощи детям в

обучении в условиях изоляции, была предварительно загружена вредоносным ПО.

Затронутые ноутбуки, распространенные в школах по схеме правительства Великобритании Get Help With Technology (GHWT), которая стартовала в прошлом году, поставлялись в комплекте с Gamarue - старым червем удаленного доступа из 2010-х годов. Это неприятное программное обеспечение не просто распространяется с компьютера на компьютер, оно также пытается подключиться к внешним серверам для выполнения инструкций.

Регистр понимает, что партия из 23000 компьютеров GeoBook 1E под управлением Windows 10, произведенная Tactus Group со штаб-квартирой в Шэньчжэне, содержала устройства, на которых было установлено вредоносное ПО. Пресс-секретарь производителя не дал комментариев.

Эти устройства были доставлены за последние три-четыре недели, хотя неясно, сколько из них заражено. Один источник в школе сообщил The Register, что рассматриваемые машины, по всей видимости, были произведены в конце 2019 года, и в прошлом году на них было установлено программное обеспечение, указанное в DfE.

Нам были показаны электронные письма, отправленные в и из Департамента образования (DfE), который курирует схему GHWT, и выражает озабоченность по поводу ноутбуков. Похоже, что по крайней мере одна школа форматирует и обновляет образы ноутбуков из известной чистой сборки в результате заражения, прежде чем выдать их ученикам.

Мы также видели онлайн-форумы, на которых сотрудники школы Брэдфорда обсуждали совет, связываясь с ними в среду, чтобы предупредить их о проблеме, говоря в электронном письме: «После распаковки и подготовки их было обнаружено, что некоторые ноутбуки заражены самим собой. -распространяющий сетевой червь ... похоже, что он связывается с российскими серверами в активном состоянии.

Люди, знакомые с развертыванием GHWT, рассказали The Register, что, однако, не все машины в партии звонили домой.

GeoBook 1E предназначены для использования школьниками, которые изолируются дома во время пандемии, а также в самих школах. Рег понимает, что 77 000 единиц Geo уже отгружены по программе GHWT, и еще несколько тысяч осталось отгрузить.

Пресс-секретарь DfE сообщила The Register: «Нам известно о проблеме с небольшим количеством устройств, и мы в первоочередном порядке занимаемся расследованием, чтобы решить эту проблему как можно скорее. ИТ-специалисты DfE связываются с теми, кто сообщил об этой проблеме. Мы считаем, что это не так широко».

Другой источник сказал о бренде Geo: «Я никогда раньше не слышал о Geo; это неизвестный производитель. Некоторое время были проблемы с доступностью, мир покупает много ноутбуков, а иногда они покупают то, что они может получить, потому что СМИ и оппозиционные партии говорят: «Вы должны развернуть это быстрее».

Источники сообщили нам, что поставщик XMA предоставил комплект, но его не просили настроить. Он был одним из трех торговых посредников, заключивших контракт с GHWT. Первоначально Computacenter заключил контракт на поставку GHWT на сумму 87 млн фунтов стерлингов в прошлом году, а позже в том же году к нему присоединились торговые посредники SCC UK и XMA. XMA подписала 12-месячный контракт на сумму 5,7 млн фунтов стерлингов на 26 449 устройств в октябре 2020 года. Сделка SCC на сумму 2,1 млн фунтов стерлингов, также подписанная в этом месяце, распространяется на еще 10 000 устройств.

XMA сообщил нам, что без комментариев.

Антивирусная компания Sophos описала Gamarue в блоге от 2016 года как «червя, обеспечивающего удаленный доступ к уязвимым системам», который обычно «распространяется через съемные диски».

«При первом запуске W32 / Gamarue-BJ подключается к сайту C2 для загрузки обновлений и дальнейших инструкций», - сказал Sophos.

Вредоносная программа, хорошо известная поставщикам антивирусных программ с момента ее появления в 2011 году, также была распространена в середине 2010-х годов ботнетом Andromeda. Это было нокаутировано международной коалицией в 2017 году. C2 Gamarue - его командно-контрольный сервер - также может быть сейчас бездействующим.

Если вас беспокоит ноутбук вашего ребенка, обратитесь за помощью в его школу. Если в GeoBook есть антивирусное программное обеспечение, обновите его (если возможно) до последней версии вручную и выполните полное сканирование системы. Это должно удалить любые следы Гамару». ***(Gareth Corfield. Laptops given to British schools came preloaded with remote-access worm // The Register (https://www.theregister.com/2021/01/21/dept_education_school_laptops_malware/). 21.01.2021).***

***

«Woodland Trust, мирная британская благотворительная организация, заботящаяся о деревьях, перед Рождеством подверглась «кибератаке».

Члены фонда, который заявляет, что с момента его основания в 1972 году посадили 43 миллиона деревьев, вчера вечером были проинформированы о том, что неизбежно описывалось как «сложный киберинцидент высокого уровня».

Может показаться не очевидным, чего киберпреступники хотели достичь, нацеливаясь на доверие, чей онлайн-контент включает руководства по посадке деревьев и тому, как возражать против приложений для планирования разрешений, которые могут привести к вырубке деревьев, - но у него есть 250 000 зарегистрированных участников.

Главный исполнительный директор Даррен Муркрофт сообщил членам Woodland Trust в электронном письме, отправленном вчера днем: «Как только нам стало известно об инциденте, мы привлекли группу внешних специалистов, которые начали расследование, а также приняли немедленные меры для смягчения последствий».

Он добавил: «Мы сообщили об инциденте в Управление комиссара по информации (ICO), комиссию по благотворительности, а также в подразделение полиции по киберпреступлениям».

Благотворительная организация в заявлении на своем веб-сайте сообщила, что «никакие данные не были скомпрометированы», о которых она знает, но при этом предупредила участников, что они должны проявлять бдительность в отношении необычных телефонных звонков или сообщений, которые могут исходить от траста или из банков.

Предполагается, что атака произошла «после 19:00 14 декабря», что, похоже, относится к первому обнаруженному вторжению в системы Woodland Trust.

В заявлении благотворительной организации говорится, что она «отключила свои ИТ-системы». Рег спросил, что это были за системы и от чего они были отключены. Пока нет информации о том, была ли атака программой-вымогателем, хотя масштабы реакции и агентства, с которыми были установлены контакты, имеют много общего с предыдущими ответами организаций Великобритании на программы-вымогатели.

Если это программа-вымогатель, атака демонстрирует, что ни одна организация, какой бы безобидной она ни была, не является закрытой, поскольку все более жадные мошенники охотятся за данными, чтобы получить прибыль. В частности, благотворительные организации обычно хранят большие объемы личных данных в виде списков участников, поэтому они могут стать следующим рубежом в вечной войне с программами-вымогателями». ***(Gareth Corfield. Today's 'sophisticated cyber attack' victim is the Woodland Trust: Pre-Xmas breach under investigation // The Register (https://www.theregister.com/2021/01/27/woodland_trust_cyber_attack/).*** 27.01.2021).

***

«Компания Palfinger, ведущий производитель кранов и подъемников, подвергается постоянной кибератаке, которая нарушила ИТ-системы и бизнес-операции.

Palfinger - ведущий производитель кранов и подъемных решений, обычно используемых в строительстве, а также наземных и морских подъемных, погрузочных и погрузочно-разгрузочных решений.

Palfinger - австрийская компания с более чем 11000 сотрудников в 35 офисах и выручкой в размере 1,75 млрд евро в 2019 году.

Palfinger пострадал от глобальной кибератаки

На сайте Palfinger в настоящее время отображается предупреждение о том, что компания подвергается кибератаке, в результате которой была отключена их электронная почта и нарушены бизнес-операции.

«В настоящее время компания PALFINGER AG и большинство ее сайтов являются целью продолжающейся глобальной кибератаки с огромными последствиями для ее ИТ-инфраструктуры. Масштабы и последствия атаки в настоящее время не могут быть оценены, но предпринимаются активные усилия. найти решение».

«В настоящее время с PALFINGER нельзя связаться по электронной почте, а также он не может получать или обрабатывать запросы, заказы, поставки и счета. Ваши личные контактные лица на этом этапе доступны только по телефону», - говорится в предупреждении на веб-сайте Palfinger.

В уведомлении о безопасности, озаглавленном «Кибератака на группу PALFINGER», также говорится, что их системы планирования ресурсов предприятия (ERP) не работают и что «затронута значительная часть местоположений группы по всему миру».

В электронном письме, увиденном BleepingComputer, Palfinger предупреждает партнеров об атаке и советует им использовать «альтернативные каналы (мобильный телефон, SMS, Whatsapp, ...)» для связи с контактами Palfinger.

Palfinger также попросил партнеров пока не создавать дальнейшие заказы на поставку.

Неизвестно, что стало причиной кибератаки, но, скорее всего, это была атака с использованием вымогателя». ***(Lawrence Abrams. Leading crane maker Palfinger hit in global cyberattack // Bleeping Computer (https://www.bleepingcomputer.com/news/security/leading-crane-maker-palfinger-hit-in-global-cyberattack/). 25.01.2021).***

***

«В четверг Intel сообщила, что неизвестные злоумышленники украли инфографику, содержащую информацию о финансовых результатах компании за четвертый квартал и полный 2020 год.

Эти данные были частью еще не опубликованной квартальной прибыли Intel, которую компания планировала опубликовать и направить в Комиссию по ценным бумагам и биржам США после закрытия фондовой биржи в четверг.

Отчет о прибылях и убытках опубликован заранее

Однако, обнаружив инцидент и обнаружив, что украденная информация распространялась за пределами компании, Intel опубликовала квартальный отчет о прибылях за несколько минут до закрытия рынка.

«Мы изучаем сообщения о том, что несанкционированный доступ мог быть получен к одному графическому изображению в нашем отчете о доходах», - сообщили BleepingComputer в Intel.

«Вчера, когда нам стало известно об этих отчетах, мы приняли решение опубликовать объявление о доходах на короткое время до первоначально запланированного времени выпуска».

Эта мера была принята, чтобы не допустить, чтобы лица, которые могли получить доступ к украденной инфографике, незаконно использовали полученную заранее информацию для получения несправедливого преимущества на рынке…

На Intel в прошлом году повлияла еще одна утечка данных, когда разработчик и реверс-инженер Тилли Коттманн в августе утекла примерно 20 ГБ конфиденциальных документов Intel, получив их от анонимного источника, который якобы взломал серверы Intel, чтобы украсть их.

Представитель Intel позже сообщил BleepingComputer, что «информация, по всей видимости, исходит из Центра ресурсов и проектирования Intel, в котором

размещена информация для использования нашими клиентами, партнерами и другими внешними сторонами, зарегистрировавшимися для доступа»…». ***(Sergiu Gatlan. Intel: Hackers stole unpublished earnings info from corporate site // Bleeping Computer (https://www.bleepingcomputer.com/news/security/intel-hackers-stole-unpublished-earnings-info-from-corporate-site/). 22.01.2021).***

***

«Исследователи проследили происхождение кампании - заражения серверов SQL для добычи криптовалюты - до иранской фирмы-разработчика программного обеспечения.

Исследователи сделали новые открытия, связанные с источником ранее открытой операции криптомайнинга, нацеленной на серверы баз данных, подключенные к Интернету.

Кампания, получившая название MrbMiner, была обнаружена в сентябре 2020 года при загрузке и установке криптомайнера на тысячи SQL-серверов. Теперь исследователи из Sophos проследили происхождение кампании до небольшой компании по разработке программного обеспечения, базирующейся в Иране.

«Название иранской компании-разработчика программного обеспечения было жестко закодировано в основном файле конфигурации майнера», - заявили исследователи из Sophos в своем анализе в четверг. «Этот домен связан со многими другими zip-файлами, также содержащими копии майнера. Эти zip-файлы, в свою очередь, были загружены с других доменов, одним из которых является mrbftp.xyz».

Исследователи заявили, что их записи не раскрывают точно, как вредоносная программа закрепилась на серверах баз данных. Однако они указали на возможные методы, используемые ботнетом MyKings для атаки SQL или ботнетом с криптовалютой Lemon_Duck. Оба этих ботнета используют различные незащищенные уязвимости в системах с некоторыми дополнительными уловками, связанными с вектором заражения (в том числе подбором пароля протокола удаленного рабочего стола для Lemon Duck).

После загрузки в систему файлы полезной нагрузки и конфигурации криптомайнера распаковываются. Процесс сервера Microsoft SQL (sqlservr.exe) сначала запускает файл с именем assm.exe, который представляет собой троян, выполняющий роль загрузчика. Затем Assm.exe загружает полезную нагрузку криптомайнера с веб-сервера и подключается к своему командному серверу (C2), чтобы сообщить об успешной загрузке и запуске майнера.

«В большинстве случаев полезной нагрузкой был файл с именем sys.dll, который (несмотря на его суффикс) был не DLL Windows, а zip-архивом, содержащим двоичный файл криптомайнера, файл конфигурации и связанные файлы», - заявили исследователи.

Ссылки

Хотя атака казалась типичной для большинства атак криптомайнера, нацеленных на серверы, подключенные к Интернету, ее отличает то, что злоумышленник, по-видимому, предупредил о сокрытии своей личности, сказал Габор Саппанос, директор по исследованию угроз Sophos Labs.

Исследователи обнаружили множество записей, относящихся к конфигурации майнера, его доменам и IP-адресам, которые указывали на одну точку происхождения: (неназванную) небольшую софтверную компанию, базирующуюся в Иране. Например, было выдано то, что сервер, используемый для размещения полезной нагрузки для кампании, также размещал домен (vihansoft.ir), который представляет собой веб-сайт, связанный с компанией-разработчиком программного обеспечения.

«Мы нашли ссылку на бизнес, стоящий за vihansoft.ir, на персидском картографическом сайте neshan.org», - сказали исследователи. «Подобно Google Maps или Waze, Neshan включает бизнес-информацию как часть своих картографических сервисов, а также запись для компании, которая указывает vihansoft.ir в качестве своего веб-сайта и называет своего управляющего директора».

Исследователи отметили, что криптоджекинг может быть использован здесь людьми, которые живут в таких странах, как Иран, которые находятся под строгими международными финансовыми санкциями США, чтобы обойти традиционную банковскую систему.

Серверы: прибыльная цель криптоджекинга

Хотя многие злоумышленники нацелены на компьютеры с помощью своего вредоносного ПО, занимающегося криптодобычей, исследователи подчеркнули, что серверы баз данных являются привлекательной целью для злоумышленников, поскольку они используются для ресурсоемких процессов и, таким образом, обладают мощными возможностями обработки.

По словам исследователей, ИТ-администраторам, размещающим базу данных, предъявляются высокие требования к производительности, включая способность обрабатывать большие объемы операций чтения и записи данных, а также высокие уровни нагрузки на ОЗУ и процессора для быстрого ответа на запросы.

«В результате серверы, на которых размещены базы данных, оказываются на более высокой стороне шкалы производительности, поэтому они являются отличной целью для злоумышленников, чьи цели включают распространение майнеров криптовалюты», - говорят исследователи.

Злоумышленники заметили это в последние годы. В 2019 году до 50000 серверов были заражены в рамках масштабной кампании криптоджекинга, которая, как считается, была организована противниками, говорящими на китайском языке. В 2018 году появился MassMiner, нацеленный на серверы Windows с различными хорошо известными эксплойтами, все в одном исполняемом файле, включая хакерский инструмент EternalBlue NSA». ***(Lindsey O'Donnell. SQL Server Malware Tied to Iranian Software Firm, Researchers Allege // Threatpost (https://threatpost.com/sql-server-malware-tied-to-iranian-software-firm-researchers-allege/163230/). 21.01.2021).***

***

«Исследователи предупреждают, что злоумышленники собирают данные о будущих атаках на электронную почту с помощью Google Forms.

Злоумышленник рассылает организациям тысячи электронных писем. Исследователи предупреждают, что это разведывательная кампания с целью выявления целей для возможной последующей атаки с использованием компрометации корпоративной электронной почты (BEC).

До сих пор исследователи наблюдали тысячи сообщений, отправленных компаниям с декабря 2020 года, в основном в секторы розничной торговли, телекоммуникаций, здравоохранения, энергетики и производства. Следует отметить, что в кампании используется инструмент опроса Google Forms. Такое использование Google Forms киберпреступниками не ново и регулярно наблюдается в фишинговых кампаниях с использованием учетных данных для обхода фильтров содержимого электронной почты. Однако в этой атаке использование Google Forms может также вызвать постоянный диалог между получателем электронной почты и злоумышленником, делая их жертвой будущей ловушки BEC, говорят исследователи.

«Эта гибридная кампания сочетает в себе преимущества масштаба и легитимности за счет использования сервисов Google с атаками социальной инженерии, которые чаще всего связаны с BEC», - отмечают исследователи Proofpoint в своем анализе в среду.

Сообщения содержат уникальные имена руководителей высшего звена из целевых организаций, что указывает на то, что киберпреступники выполнили свою домашнюю работу, когда дело доходит до точного определения жертв. Сами сообщения «просты, но передают ощущение срочности», - сказали исследователи - они спрашивают жертву, есть ли у них «быстрый момент» для выполнения задачи, поскольку предполагаемый отправитель якобы направляется на встречу или слишком занят, чтобы справиться сами задачи и укажите ссылку в письме.

Эта ссылка ведет жертву к форме по умолчанию без названия, размещенной в инфраструктуре Google Forms. Google Forms - это программное обеспечение для администрирования опросов, которое предлагается как часть пакета Google Doc Editors. Как ни странно, форма в этой кампании пуста, а просто написано «Форма без названия» с «Вопросом без названия».

Исследователи считают, что основная цель состоит в том, чтобы получить от жертвы ответ по электронной почте, чтобы сообщить, что опрос не соответствует ожиданиям. Это может привести к дальнейшему диалогу между жертвой и атакующим, заложив основу для будущей атаки BEC.

«В качестве второстепенной цели форма, вероятно, служит датчиком, чтобы просто увидеть, заполняет ли кто-нибудь свою форму, действуя как метод разведки, чтобы отсеять пользователей, которые могут быть восприимчивы к нажатию на подозрительную ссылку, найденную в электронном письме», - сказали исследователи.

Несмотря на этот трюк, у самих электронных писем есть несколько красных флажков, которые могут служить мертвой раздачей для подозрительного получателя электронной почты. Сюда входят ошибочные орфографические и грамматические ошибки, в одном сообщении говорится: «Является ли ваше расписание гибким, чтобы выполнять задачу для меня сейчас, = m, направляясь на

встречу, теперь не может принимать звонки или текстовые сообщения, просто отправьте меня обратно».

Еще одна раздача - это адреса электронной почты злоумышленников, используемые в этой кампании, которые в некоторых случаях вообще не имеют никакого сходства с законными (например, fgtytgyg [@] gmail.com).

«Мы не наблюдали установленной закономерности в поддельных электронных письмах; однако некоторые из адресов выглядят так, как будто они были созданы с помощью случайного набора клавиш, в то время как другие содержат общие имена / фразы, - сказал Threatpost Шеррод ДеГриппо, старший директор по исследованию и обнаружению угроз в Proofpoint.

Исследователи полагают, что это только начало кампании - по их словам, злоумышленники могут собирать данные разведки, чтобы определить цели для неопределенных последующих действий по угрозам.

«Настроение срочности в электронных письмах соответствует предыдущим участникам BEC, и поэтому мы хотим обеспечить осведомленность о безопасности этих попыток как указание или предупреждение для клиентов и сообщества безопасности», - заявили исследователи.

Злоумышленники ранее использовали службы Google, в том числе Google Forms, различными вредоносными способами. Одна из фишинговых атак в ноябре использовала Google Forms в качестве целевой страницы для сбора учетных данных жертв, при этом формы маскировались под страницы входа от более чем 25 различных компаний, брендов и государственных учреждений. Другая ноябрьская кампания использовала Google Form и логотип American Express, чтобы попытаться убедить жертв ввести конфиденциальную информацию. Также в ноябре мошенники использовали законную функцию совместной работы на Google Диске, чтобы заставить пользователей переходить по вредоносным ссылкам.

«Хотя социальная инженерия широко распространена во всех атаках, связанных с электронной почтой, в случае фишинга вредоносных программ и учетных данных она используется иначе, чем в кампаниях BEC», - говорят исследователи Proofpoint. «В кампании вредоносных программ в исходном письме используется социальная инженерия. И наоборот, в BEC социальная инженерия используется на протяжении всего жизненного цикла мошенничества. Хотя это редко, мы наблюдаем, как злоумышленники доставляют вредоносные программы после обмена безопасными сообщениями». ***(Lindsey O'Donnell. Google Forms Set Baseline For Widespread BEC Attacks // Threatpost (https://threatpost.com/google-forms-set-baseline-for-widespread-bec-attacks/163223/). 21.01.2021).***

***

«Специалисты FireEye Email Security зафиксировали волну фишинговых атак на пользователей в Европе, Северной и Южной Америке, в ходе которых злоумышленники используют обфускацию вредоносного кода с помощью шифра подстановки на базе WOFF и Telegram-каналы для связи.

Атака начинается с получения жертвой электронного письма, замаскированного под уведомление от службы экспресс-доставки DHL. В письме содержится ссылка на поддельный сайт DHL с фишинговой формой, куда жертва

должна ввести данные своей банковской карты, которые затем отправляются прямиком киберпреступникам.

По словам экспертов, в данной кампании злоумышленники используют весьма редкий метод обфускации исходного кода страницы. Исходный код страницы содержит надлежащие строки и действительные теги и отформатирован должным образом. Однако в нем также содержится текст, закодированный с помощью шифра подстановки и напоминающий бессмысленный набор символов.

Как правило, скрипт для дешифровки таких текстов встраивается в сам код страницы, однако в данном случае он отсутствует. Декодирование текста осуществляется с помощью файла шрифтов Web Open Font Format (WOFF) во время загрузки страницы, и процесс расшифровки не виден жертве. Загрузка декодирующего текст кастомизированного шрифта выполняется внутри каскадных таблиц стилей (CSS). Этот метод встречается редко, так как для шифрования и дешифрования HTML- текстов обычно используется JavaScript.

Стоящие за фишинговой кампанией злоумышленники охотятся за учетными данными пользователей, данными их кредитных карт и другой конфиденциальной информацией. Похищенные с помощью поддельных форм сведения отправляются на подконтрольные им адреса электронной почты и Telegram-каналы. В частности, исследователи обнаружили Telegram-канал, на которой данные отправляются с помощью Telegram Bot API». ***(Фишеры вооружились редкими методами обфускации и Telegram-каналами // SecurityLab.ru (https://www.securitylab.ru/news/515991.php). 27.01.2021).***

***

«Специалисты регионального интернет-регистратора African Network Information Centre (AfriNIC) Африки опубликовали отчет о внутреннем расследовании кражи больших объемов интернет-ресурсов соучредителем организации. По результатам расследования, в общей сложности было незаконно присвоено более 4,1 миллиона IP-адресов — 2,3 млн из «бесплатного пула» AfriNIC и еще 1,7 млн «старых» IP-адресов.

О внутренней проблеме стало известно только в 2019 году после уведомления от Федерального бюро расследований США (ФБР) о подозрительных действиях в отношении нескольких блоков адресов IPv4.

По некоторым оценкам, один адрес IPv4 продается на рынке реселлеров примерно за $20. При цене 15 южноафриканских рэндов за $1 общая стоимость скомпрометированных блоков IP-адресов составляет около 1,25 млрд рандов (около $82,5 млн).

Блоки IP-адресов были незаконно присвоены путем манипулирования их записями в базе данных AfriNIC WHOIS. WHOIS представляет собой сетевой протокол прикладного уровня, базирующийся на протоколе TCP. Основное применение — получение регистрационных данных о владельцах доменных имен, IP-адресов и автономных систем.

«Предварительное расследование, проведенное внутри организации, также показало, что внутренний персонал мог без каких-либо законных полномочий действовать в сговоре с другими третьими сторонами», — заявили в AFRINIC».

(Злоумышленник похитил 4,1 млн IP-адресов AfriNIC на сумму $82 млн // SecurityLab.ru (https://www.securitylab.ru/news/515997.php). 27.01.2021).

***

«Команда ИБ-специалистов Threat Analysis Group компании Google выявила текущую кампанию, нацеленную на исследователей безопасности, которые изучают уязвимости в ПО. По словам экспертов, кампания продолжается уже несколько месяцев, а за атаками стоит «поддерживаемая правительством организация, базирующаяся в Северной Корее». Преступники обычно используют социальную инженерию, чтобы вызвать доверие у жертв.

Злоумышленники создают собственные исследовательские блоги, в которых публикуют анализ известных уязвимостей, выдавая себя за легитимных экспертов. Хакеры также ведут учетные записи в Twitter и публикуют видеозаписи заявленных ими исследований, привлекая как можно больше людей. В одном случае специалисты Google обнаружили, хакеры поделились в Twitter видеороликом с YouTube с якобы успешной эксплуатацией уязвимости в Windows Defender (CVE-2021-1647). Когда под видео стали появляться комментарии, что эксплоит не работает, они создали еще одну учетную запись в Twitter, с которой написали, что видео не фальшивое.

Злоумышленники отправляли сообщения своим предполагаемым жертвам и просили помочь им в исследовании уязвимостей. Помимо Twitter, они также используют LinkedIn, Telegram, Discord, Keybase и электронную почту, чтобы связываться со своими целями и отправлять им проект Microsoft Visual Studio с вредоносным ПО. В некоторых случаях компьютеры жертв были взломаны после посещения блога злоумышленников после перехода по ссылке в Twitter. Оба метода приводили к установке на компьютерах жертв бэкдора, который подключал их к управляемому злоумышленниками C&C-серверу.

Системы жертв были скомпрометированы при наличии полностью исправленных и современных версий Windows 10 и браузера Chrome. Команда Google TAG призывает исследователей отправлять уязвимости в Chrome в рамках программы вознаграждения за обнаружение проблем». ***(Северокорейские хакеры выдают себя за ИБ-экспертов для распространения вредоносов // SecurityLab.ru (https://www.securitylab.ru/news/515966.php). 26.01.2021).***

***

«Спуфинг (от англ. spoofing) – это кибер-атака, в рамках которой мошенник выдает себя за какой-либо надежный источник, чтобы получить доступ к важным данным или информации. Такая подмена (спуфинг-атака) может происходить через веб-сайты, электронную почту, телефонные звонки, текстовые сообщения, IP-адреса и серверы.

Как правило, основная цель спуфинга – получить доступ к личной информации, украсть деньги, обойти контроль доступа к сети или распространить вредоносное ПО через ссылки на зараженные веб-страницы или зараженные файлы, вложенные в электронное письмо или сообщение. При любой форме

общения в Интернете мошенники будут пытаться использовать спуфинг, чтобы попытаться украсть чужую онлайн-личность и ИТ-активы.

Как происходит спуфинг

Термин «spoof» (спуф) в английском языке существует уже более века и относится к любой форме обмана. Однако сегодня он в основном используется в тех случаях, когда речь идет о кибер-преступности. Каждый раз, когда мошенник маскируется под другого человека (организацию, сайт, отправитель и пр.), мы имеем дело со спуфингом.

Спуфинг может применяться к различным коммуникационным каналам и задействовать различные уровни технических ноу-хау. Чтобы спуфинг-атака была успешной, она должна включать в себя определенный уровень социальной инженерии. Это означает, что методы, которые используют мошенники, способны обмануть жертву и заставить ее предоставить свою личную информацию. Мошенники используют методы социальной инженерии, чтобы играть на уязвимых человеческих качествах, таких как жадность, страх и наивность.

Примером такого типа социальной инженерии является случай, когда мошенник полагается на чувство страха жертвы в попытке заполучить от него информацию или деньги. Мошенничество с внуками – это когда мошенник притворяется членом семьи (внуком) и якобы заявляет жертве (бабушке или дедушке этого внука), что у него неприятности и ему срочно нужны деньги. Мошенники часто нацеливаются в таких ситуациях именно на пожилых людей из-за предвзятого представления о том, что пожилые люди менее технически грамотны…

Спуфинг с подменой номера вызывающего абонента

Идентификатор вызывающего абонента (Caller ID) позволяет получателю телефонного звонка определить личность того, кто звонит. Такой вид спуфинга происходит в тех случаях, когда мошенник использует ложную информацию для изменения идентификатора вызывающего абонента (т.е. мошенник звонит якобы с другого телефона). Поскольку спуфинг с подменой идентификатора вызывающего абонента делает невозможной блокировку номера, многие мошенники используют такой вид спуфинга, чтобы скрыть свой реальный номер телефона, с которого осуществляется звонок, чтобы в конечном итоге скрыть свою личность.

Большинство спуфинг-атак с подменой идентификатора вызывающего абонента происходит с помощью VoIP (Voice over Internet Protocol), который позволяет мошенникам создавать номер телефона и имя идентификатора вызывающего абонента по своему выбору. Как только получатель звонка ответит на звонок, мошенник попытается убедить его предоставить ему требуемую важную информацию.

Спуфинг с подменой сайта

Это тип спуфинг-атаки, в рамках которой мошенник старается сделать опасный (вредоносный) сайт похожим на надежный безопасный сайт (например, известного банка), используя его шрифты, цвета и логотипы. Такой спуфинг проводится путем репликации оригинального надежного сайта с целью привлечения пользователей на специально созданный поддельный фишинговый или вредоносный сайт. Такие «скопированные» сайты, как правило, имеют

примерно такой же адрес сайта, как и исходный оригинальный сайт, а потому, на первый взгляд, кажутся обычным пользователям реальными (оригинальными) сайтами. Однако такие «скопированные» сайты обычно создаются для незаконного получения личной информации посетителя сайта.

Спуфинг с подменой адреса электронной почты

Это тип спуфинг-атаки, в рамках которой мошенник рассылает электронные письма с поддельными адресами отправителей с намерением заразить компьютер жертвы вредоносными программами, заполучить деньги или украсть информацию. В качестве адресов электронной почты отправителей зачастую подставляются те адреса, которым могут доверять (коллега по работе, друг, родственник, банк и т.д.).

Также в качестве адресов электронной почты отправителей могут подставляться те адреса, которые очень похожи на адреса известных отправителей (незаметная разница в букве/ цифре), либо мошенник может маскировать поле «От» («From») с адресом отправителя и в точности указывать тот адрес электронной почты, которому могут доверять.

Спуфинг с подменой IP-адреса

Когда мошенник стремится скрыть реальное местоположение в Интернете того места, откуда запрашиваются или куда отправляются данные пользователя/ жертвы, то обычно используется спуфинг с подменой IP-адреса. Цель IP-спуфинга состоит в том, чтобы заставить компьютер жертвы думать, что информация, отправляемая мошенником пользователю, исходит из надежного источника, что позволяет вредоносному контенту доходить до пользователя.

Спуфинг с подменой DNS-сервера

Также известный как «отравление кэша», используется для перенаправления трафика пользователя на поддельные IP-адреса. Такой метод позволяет перенаправлять пользователей на вредоносные сайты. В рамках такой атаки мошенник меняет IP-адреса DNS-серверов, указанных на компьютере жертвы, на поддельные IP-адреса, который мошенник хочет использовать для обмана жертвы.

ARP-спуфинг

ARP-спуфинг (Address Resolution Protocol) часто используется для изменения или кражи данных, а также для взлома компьютера жертвы внутри его сессии (подключения). Для этого злоумышленник свяжет себя с IP-адресом жертвы, чтобы иметь возможность получить доступ к тем данным, которые изначально предназначались для владельца этого IP-адреса (т.е. жертвы).

SMS-спуфинг

Спуфинг с подменой текстовых сообщений (известен также как SMS-спуфинг) – это тип спуфинг-атаки, в рамках которой мошенник отправляет текстовое или SMS-сообщение, используя номер телефона другого человека. Мошенники делают это, скрывая свою личность за буквенно-цифровым идентификатором отправителя, и обычно в свои сообщения включают ссылки для загрузки вредоносных программ или для перехода на фишинговые сайты.

GPS-спуфинг

Атака типа GPS-спуфинг происходит для «обмана» GPS-приемника, когда передаются поддельные сигналы, которые напоминают настоящие. Другими словами, мошенник притворяется, что находится в одном месте, а на самом деле

находится в другом. Мошенники могут использовать такой прием, чтобы, например, взломать GPS в автомобиле и направить водителя по ложному адресу или даже вмешаться в GPS-сигналы кораблей, самолетов и т.д. Любое мобильное приложение, которое полагается на данные о местоположении смартфона, может стать мишенью для такого типа атаки.

Атака посредника или «человека посередине» (Man-in-the-middle Attack, MitM)

Атаки типа Man-in-the-middle (MitM) происходят в тех случаях, когда мошенник взламывает Wi-Fi сеть или создает дублирующую поддельную Wi-Fi сеть в том же месте для перехвата веб-трафика между двумя сторонами подключения (отправитель и получатель трафика). С помощью такой атаки мошенники могут перенаправлять к себе используемую жертвой конфиденциальную информацию, такую как логины, пароли или номера банковских карт.

Спуфинг с подменой расширений файлов

Чтобы замаскировать вредоносные программы, мошенники часто используют спуфинг с подменой расширений. Например, они могут переименовать файл в «filename.txt.exe», спрятав вредоносную программу внутри расширения. Таким образом, файл, который кажется текстовым документом, на самом деле при его открытии запускает вредоносную программу…

Спуфинг с подменой адреса электронной почты

Обратите внимание на адрес отправителя: если вы не уверены, является ли полученное вами письмо подлинным, дважды проверьте адрес. Мошенники часто создают похожие адреса. Если это подозрительное письмо, но при этом указан правильный адрес электронной почты отправителя, то отдельно свяжитесь с этим отправителем, например в мессенджере или по телефону, чтобы подтвердить аутентичность его письма.

Следует быть особенно осторожным, когда речь идет о вложениях в электронное письмо от неизвестного отправителя или даже от известного отправителя в том случае, если содержимое выглядит подозрительным. Если вы сомневаетесь, не открывайте такие вложения, так как они могут содержать вирусы и другие вредоносные программы.

Обратите внимание на плохую грамматику: если письмо содержит необычные грамматические ошибки и опечатки, оно может быть вредоносным

Проведите небольшое исследование: найдите контактную информацию отправителя в Интернете и свяжитесь с ним напрямую, чтобы узнать, является ли письмо реальным. Кроме того, поищите содержимое письма через поисковик (например, Google), если оно кажется подозрительным. Как правило, если содержание письма выглядит слишком заманчивым, чтобы быть правдой, то это может свидетельствовать о мошенническом характере письма.

Спуфинг с подменой сайта

Проверьте адресную строку в вашем браузере: поддельный веб-сайт, скорее всего, не будет защищен. Сайты, использующие протокол https:// с шифрованием, как правило, лучше защищены от кибер-преступников. Отсутствие буквы «s» в

начале адреса не обязательно означает, что сайт поддельный. Но это повод проявить бдительность и проверить дополнительные признаки.

Используйте менеджер паролей: программное обеспечение, используемое для автоматического заполнения регистрационных данных для авторизации, не работает на поддельных веб-сайтах. Если ПО автоматически не заполняет поля с паролем и именем пользователя, то такое поведение менеджера паролей может быть признаком поддельного веб-сайта.

Отсутствие символа с замочком: легитимные веб-сайты имеют символ замочка или зеленую полосу слева от URL-адреса веб-сайта, указывающую на безопасность данного веб-сайта.

Спуфинг с подменой номера вызывающего абонента

Вы получаете звонки с неизвестных номеров: настойчивые звонки с неизвестного номера обычно являются признаком спуфинга. В этом случае не отвечайте на такие звонки или не поднимайте трубку сразу же.

Вы получаете странные ответы: если вы получаете ответы на звонки или сообщения, которые вы никогда не делали, это может быть признаком того, что ваш номер был подделан. Например, вы можете получать текстовые сообщения от людей, которые спрашивают, кто вы, зачем вы им звонили, почему вы их беспокоите и пр.

Номер вызывающего абонента показывает номер спецслужбы: иногда вместо номера вызывающего абонента может отображаться номер какой-либо из специальных служб вместо фактического, реального номера телефона вызывающей стороны.

Как защититься от спуфинг-атак

Чтобы защититься от спуфинг-атак, специалисты рекомендуют придерживаться ряда рекомендаций.

СЛЕДУЕТ ДЕЛАТЬ

Включите спам-фильтр: это предотвратит попадание большинства поддельных писем в ваш почтовый ящик.

Изучите сообщение: если потенциальная спуфинг-атака содержит признаки плохой грамматики или необычной структуры предложения, это может свидетельствовать о незаконном характере сообщения. Кроме того, не забудьте дважды проверить URL-адрес веб-сайта или адрес отправителя электронной почты.

Подтвердите информацию: если электронное письмо или звонок кажутся подозрительными, отправьте сообщение или отдельно позвоните отправителю, чтобы проверить, является ли полученная вами информация достоверной или нет. Если письмо или звонок были сделаны якобы от какой-то организации, попробуйте в Интернете найти ее сайт или номер телефона, чтобы проверить эту информацию на сайте или в их контакт-центре.

Наведите указатель мыши перед кликом на ссылку: если URL-адрес выглядит подозрительно, наведите курсор мыши на ссылку, чтобы точно увидеть, куда приведет вас ссылка, прежде чем нажать на нее.

Настройте двухфакторную авторизацию: это хорошая возможность добавить еще один уровень защиты к вашим данным доступа. Однако это не является 100%

защитой, а потому убедитесь, что вы также используете и другие меры предосторожности.

Используйте антивирусное ПО: установка ПО для информационной безопасности – это разумное решение, когда дело доходит до защиты от мошенников в Интернете. Если у вас возникли проблемы, скачайте программу для удаления данного вредоноса или антивирусное ПО, чтобы защитить компьютер от любых вредоносных угроз или вирусов.

НЕ СЛЕДУЕТ ДЕЛАТЬ

Не нажимайте на незнакомые ссылки: Если ссылка выглядит подозрительной, воздержитесь от нажатия на нее. Если она пришла от потенциального злоумышленника, то это может привести к загрузке вредоносной программы или других вирусов, которые могут заразить ваш компьютер.

Не отвечайте на электронные письма или звонки от неизвестных отправителей: если отправитель неузнаваем, не отвечайте на звонок или электронное письмо. Это может помочь предотвратить любое общение с потенциальным мошенником.

Не разглашайте личную информацию: избегайте разглашения вашей личной и конфиденциальной информации (например, номер банковской карты, соцстрахования, логины и пароли и т.д.), если вы не уверены, что общаетесь с надежным источником.

Не используйте один и тот же пароль: создайте для всех своих аккаунтов разные и надежные пароли, которые мошенникам будет труднее угадать. Часто меняйте их на случай, если мошенник завладеет одним из них. Кроме того, избегайте использования одного и того же пароля для большинства ваших аккаунтов». ***(Евгений Куликов. О спуфинге и борьбе с ним // Компьютерное Обозрение (https://ko.com.ua/o_spufinge_i_borbe_s_nim_136079). 26.01.2021).***

***

Діяльність хакерів та хакерські угруповування

«Согласно отчету, опубликованному на этой неделе, северокорейская хакерская группа Thallium атаковала пользователей частной службы обмена сообщениями об инвестициях в акции в ходе атаки на цепочку поставок программного обеспечения.

До сих пор группа в основном полагалась на фишинговые атаки, например, с использованием документов Microsoft Office, для нацеливания на своих жертв.

В настоящее время Thallium использует несколько способов, таких как отправка испорченных установщиков Windows и загруженных макросами документов Office для охоты на инвесторов.

Злоумышленники изменяют установщик приложения для инвестиций в акции

На этой неделе Центр реагирования на безопасность ESTsecurity (ESRC) сообщил о том, что северокорейская хакерская группа изменила приложение для обмена сообщениями об инвестициях в частные акции для отправки вредоносного кода.

Группа, известная как Thallium, создала исполняемый файл Windows с помощью Nullsoft Scriptable Install System (NSIS), популярного инструмента для создания установщиков, основанных на сценариях, для Microsoft Windows.

Исполняемый файл содержал вредоносный код в дополнение к легитимным файлам из законной прикладной программы для инвестирования в акции.

Исследователи ESTsecurity продемонстрировали, по крайней мере, два способа использования злоумышленниками техники «обработки сценария XSL».

В рамках законного установщика платформы для инвестиций в акции злоумышленники вводили определенные команды, которые извлекали вредоносный сценарий XSL с поддельного FTP-сервера и запускали его в системах Windows с помощью встроенной утилиты wmic.exe.

Полученный установщик, перекомпонованный с NSIS от Nullsoft, создавал впечатление, как если бы пользователь устанавливал реальное приложение для инвестирования в акции, тихо запуская вредоносные сценарии в фоновом режиме.

На следующем этапе атаки выполняется сценарий VBScript для создания файлов и папок с названиями «OracleCache», «PackageUninstall» и «USODrive» среди прочих в каталоге% ProgramData%.

Затем полезная нагрузка подключается к серверу управления и контроля (C2), размещенному на frog.smtper [.] Co, для получения дополнительных команд.

Создавая мошенническую запланированную задачу, называемую активацией, в вводящем в заблуждение каталоге «Office 365 __ \ Windows \ Office», вредоносная программа обеспечивает постоянство, инструктируя планировщик Windows запускать отброшенный код каждые 15 минут.

Злоумышленники проводят разведку зараженной системы и после первоначальной проверки развертывают на машине трояна удаленного доступа (RAT) для дальнейшего выполнения своих зловещих действий.

Макросы Excel также используются для доставки полезной нагрузки

Исследователи ESTsecurity также наблюдали документы Microsoft Office, такие как электронные таблицы Excel, содержащие макросы, которые распространяли вышеупомянутую полезную нагрузку сценария XSL.

«ESRC обращает внимание на тот факт, что организация Thallium использует технику «XSL Script Processing» не только для целевых фишинговых атак, основанных на вредоносных документах, но и для нишевых атак, включая атаки на цепочки поставок», - заявили исследователи ESTsecurity в своем переведенном отчете.

По словам исследователей, причины, по которым злоумышленники нацелены на пользователей, инвестирующих в акции, остаются неясными.

Независимо от того, была ли целью этой атаки была денежная выгода или шпионаж за трейдерами, атаки на цепочки поставок стали в наше время обычной неприятностью.

Недавняя крупномасштабная атака SolarWinds затронула более 18 000 организаций, включая авторитетные государственные и частные организации.

В прошлом месяце злоумышленники нацелились на экосистему с открытым исходным кодом RubyGems в ходе атаки на цепочку поставок программного обеспечения, чтобы украсть криптовалюту с зараженных машин». ***(Ax Sharma.***

North Korean software supply chain attack targets stock investors // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/north-korean-software-supply-chain-attack-targets-stock-investors/). 05.01.2021).

***

«Иранская кибершпионажная группа, известная как Charming Kitten (APT35 или Phosphorus), использовала недавние зимние каникулы для атаки на цели со всего мира с помощью очень сложной кампании целевого фишинга, которая включала не только атаки по электронной почте, но и SMS-сообщения.

«Charming Kitten в полной мере воспользовался этим временем, чтобы провести свою новую кампанию с максимальным эффектом», - сказала CERTFA, организация по кибербезопасности, специализирующаяся на отслеживании иранских операций.

«Группа начала новый раунд атак в то время, когда большинство компаний, офисов, организаций и т. Д. Были либо закрыты, либо наполовину закрыты во время рождественских праздников, и в результате их отделы технической поддержки и ИТ не могли немедленно проверить, выявить и нейтрализовать эти киберинциденты», - добавил он.

CERTFA сообщила, что обнаружила атаки, нацеленные на членов аналитических центров, центров политических исследований, университетских профессоров, журналистов и активистов-экологов.

Жертвы находились в странах Персидского залива, в Европе и США.

КАК РАЗВОРАЧИВАЛАСЬ АТАКА

Исследователи CERTFA заявили, что эта конкретная кампания демонстрирует высокую степень сложности. Жертвы получали целевые фишинговые сообщения от злоумышленников не только по электронной почте, но и по SMS - каналу, который не многие злоумышленники используют на регулярной основе.

В то время как SMS-сообщения выдавались за предупреждения системы безопасности Google, в электронных письмах использовались ранее взломанные учетные записи и пытались сыграть на праздничном настроении с помощью праздничных приманок.

Общим знаменателем обеих кампаний было то, что операторам Charming Kitten удалось успешно скрыть свои атаки за законным URL-адресом Google https://www.google [.] Com / url? Q = https: //script.google.com/xxxx, что могло бы обмануть даже самых технически подкованных получателей.

Но за капотом CERTFA заявил, что законный URL-адрес Google в конечном итоге приведет к тому, что пользователя перебросят через разные веб-сайты и, в конечном итоге, он попадет на фишинговую страницу, где им будет предложено ввести учетные данные для входа в личные почтовые службы, такие как Gmail, Yahoo и Outlook, но и деловые письма.

Команда CERTFA отметила, что это не первый случай, когда Charming Kitten удалось успешно скрыть ссылки на целевые фишинговые сайты за URL-адресами Google.

Компания ссылается на предыдущий отчет от января 2020 года, разоблачающий операцию Charming Kitten, в которой использовались ссылки на сайтах site.google.com». ***(Catalin Cimpanu. Iranian cyberspies behind major Christmas SMS spear-phishing campaign // ZDNet (https://www.zdnet.com/article/iranian-cyberspies-behind-major-christmas-sms-spear-phishing-campaign/). 13.01.2021).***

***

«Google заявил сегодня, что хакерская группа правительства Северной Кореи нацелена на членов сообщества кибербезопасности, занимающихся исследованиями уязвимостей.

Атаки были обнаружены Google Threat Analysis Group (TAG), группой безопасности Google, специализирующейся на поиске групп сложных постоянных угроз (APT).

В опубликованном сегодня отчете Google говорится, что хакеры из Северной Кореи использовали несколько профилей в различных социальных сетях, таких как Twitter, LinkedIn, Telegram, Discord и Keybase, чтобы связаться с исследователями безопасности, используя вымышленные личности.

По словам Google, в некоторых случаях также использовалась электронная почта.

«После установления первоначального взаимодействия участники спрашивают целевого исследователя, хотят ли они совместно работать над исследованием уязвимостей, а затем предоставляют исследователю проект Visual Studio», - сказал Адам Вайдеманн, исследователь безопасности из Google TAG.

Проект Visual Studio содержал вредоносный код, который устанавливал вредоносное ПО в операционной системе целевого исследователя. Вредоносная программа действовала как бэкдор, связываясь с удаленным сервером управления и контроля и ожидая команд.

Позже это вредоносное ПО было связано с Lazarus Group, известной северокорейской государственной операцией.

Но Видеманн сказал, что злоумышленники не всегда распространяли вредоносные файлы по своим целям. В некоторых других случаях они просили исследователей безопасности посетить блог, который они вели на blog [.] Br0vvnn [.] Io (не открывать).

Google заявил, что в блоге размещен вредоносный код, который заразил компьютер исследователя безопасности после доступа к сайту.

«В системе исследователя была установлена вредоносная служба, и бэкдор в памяти должен был передавать сигнал на сервер управления и контроля, принадлежащий субъекту», - сказал Вайдеманн.

Но Google TAG также добавил, что многие жертвы, которые обращались к сайту, также использовали «полностью исправленные и обновленные версии браузера Windows 10 и Chrome» и по-прежнему заражались.

Подробная информация об атаках через браузер по-прежнему скудна, но некоторые исследователи безопасности считают, что северокорейская группа,

скорее всего, использовала комбинацию уязвимостей нулевого дня Chrome и Windows 10 для развертывания своего вредоносного кода.

В результате команда Google TAG в настоящее время просит сообщество кибербезопасности поделиться более подробной информацией об атаках, если какие-либо исследователи безопасности считают, что они были заражены.

Отчет Google TAG включает в себя список ссылок на поддельные профили в социальных сетях, которые северокорейский актер использовал, чтобы заманить и обмануть членов сообщества информационной безопасности.

Исследователям безопасности рекомендуется просмотреть свою историю просмотров и посмотреть, взаимодействовали ли они с каким-либо из этих профилей или обращались ли они к вредоносному домену blog.br0vvnn.io.

В этом случае они, скорее всего, были инфицированы, и необходимо предпринять определенные шаги для исследования их собственных систем.

Причина нападения на исследователей безопасности довольно очевидна, поскольку это может позволить северокорейской группе украсть эксплойты для уязвимостей, обнаруженных зараженными исследователями, уязвимостей, которые группа угроз может использовать в своих собственных атаках с небольшими затратами на разработку или вообще без них.

Тем временем несколько исследователей безопасности уже сообщили в социальных сетях, что они получали сообщения от учетных записей злоумышленников, хотя ни один из них не признал, что системы были скомпрометированы». ***(Catalin Cimpanu. Google: North Korean hackers have targeted security researchers via social media // ZDNet (https://www.zdnet.com/article/google-north-korean-hackers-have-targeted-security-researchers-via-social-media/). 26.01.2021).***

***

Вірусне та інше шкідливе програмне забезпечення

«Кампания по спаму, нацеленная на более чем 100 000 пользователей в день в период Рождества и Нового года, показала, что Emotet занял свое место в качестве самой распространенной вредоносной угрозы.

Анализ, проведенный компанией Check Point, занимающейся кибербезопасностью, показывает, что в декабре Emotet использовался против 7% организаций по всему миру.

Emotet активен с 2014 года и регулярно обновляется его авторами для поддержания его эффективности. Вредоносная программа начала свою жизнь как банковский троян, но впоследствии превратилась в нечто большее, предоставляя полный бэкдор на скомпрометированные машины, который затем можно продать другим киберпреступникам для заражения жертв дополнительными вредоносными программами, включая программы- вымогатели.

Хотя Emotet обладает червеобразными возможностями, которые позволяют ему перемещаться на другие машины в той же сети, что и первоначальная жертва, он также распространяется с помощью фишинговых писем. Но независимо от того,

как это происходит, Emotet отлично справляется с сохранением настойчивости, а также избегает обнаружения, а это означает, что жертвы часто не догадываются, что их взломали, пока не станет слишком поздно.

«Изначально Emotet был разработан как банковское вредоносное ПО, которое проникало на компьютеры пользователей для кражи частной и конфиденциальной информации. Однако со временем оно эволюционировало и теперь рассматривается как один из самых дорогостоящих и разрушительных вариантов вредоносного ПО», - сказала Майя Горовиц, директор аналитики угроз и исследований в Check Point.

«Совершенно необходимо, чтобы организации знали об угрозе, которую представляет Emotet, и чтобы у них были надежные системы безопасности, чтобы предотвратить серьезную утечку их данных. Они также должны провести всестороннее обучение сотрудников, чтобы они могли определять типы вредоносных электронных писем. которые распространяют Emotet ", - добавила она.

Банковский троян Trickbot является второй наиболее распространенной формой вредоносного ПО на пороге 2021 года. Как и Emotet, он постоянно обновляется новыми возможностями и функциями, в том числе возможностью настраивать вредоносное ПО, которое позволяет использовать его во всех видах кампаний по кибер-вторжению. Как и Emotet, Trickbot стал чем-то большим, чем просто банковским трояном, и его часто устанавливают в системы в качестве шлюза для установки программ-вымогателей.

Formbook вредоносных программ для сбора учетных данных занял третье место среди наиболее обнаруживаемых вредоносных угроз за отчетный период. Formbook продается на форумах даркнета по относительно низкой цене, но предоставляет киберпреступникам все необходимое для мощной кампании по краже информации; он собирает имена пользователей и пароли из браузеров, собирает снимки экрана, отслеживает и регистрирует нажатия клавиш и многое другое.

По данным Check Point, каждая из кампаний Trickbot и Formbook была обнаружена в попытках проникнуть в сети 4% организаций по всему миру.

Другие видные вредоносные программы в декабре включены Dridex трояном, XMRig криптовалюта мин ИНГ вредоносных программ и Hiddad Android вредоносных программ…». ***(Danny Palmer. Cybersecurity: This 'costly and destructive' malware is the biggest threat to your network // ZDNet (https://www.zdnet.com/article/cybersecurity-this-costly-and-destructive-malware-is-the-most-prolific-threat-to-your-network/). 08.01.2021).***

***

«Новая фишинговая кампания пытается заманить жертв в загрузку вредоносного ПО, которое дает киберпреступникам полный контроль над зараженными компьютерами с Microsoft Windows.

Троян Quaverse Remote Access (QRat) впервые появился в 2015 году и до сих пор остается успешным, поскольку его сложно обнаружить на нескольких уровнях

обфускации, и он предоставляет злоумышленникам удаленный доступ к компьютерам скомпрометированных жертв.

Возможности этого троянского вредоносного ПО включают кражу паролей, ведение кейлоггеров, просмотр файлов, создание снимков экрана и многое другое, что позволяет хакерам получить доступ к конфиденциальной информации.

Теперь исследователи кибербезопасности из Trustwave определили новую кампанию QRat, которая пытается соблазнить людей загрузить последнюю версию вредоносного ПО, что они описывают как «значительно улучшенное».

В первоначальном фишинговом письме заявлено, что жертве предлагается ссуда с «хорошей окупаемостью инвестиций», которая потенциально может привлечь внимание жертв. Тем не менее, вредоносное вложение не имеет никакого отношения к теме фишингового письма, а утверждает, что содержит видео президента Дональда Трампа.

Исследователи предполагают, что злоумышленники выбрали это приложение на основе того, что в настоящее время заслуживает внимания. Какой бы ни была причина, попытка открыть файл - файл Java Archive (JAR) - приведет к запуску установщика вредоносного ПО QRat.

Вредоносная программа использует несколько уровней обфускации, чтобы избежать обнаружения как вредоносная деятельность, а также добавила новые методы, чтобы предоставить дополнительные средства предотвращения обнаружения.

Тем не менее, этот процесс даже сопровождается всплывающим предупреждением, сообщающим пользователю, что устанавливаемое им программное обеспечение может использоваться для удаленного доступа и тестирования на проникновение - если пользователь соглашается, этот QRat загружается в систему с извлечением вредоносного ПО. путем модульной загрузки, чтобы избежать обнаружения.

SEE: выигрышная стратегия кибербезопасности (специальный отчет ZDNet) | Скачать отчет в формате PDF (TechRepublic)

Может показаться странным, что люди соглашаются на это, когда это кажется не связанным с предполагаемым видео, к которому они пытаются получить доступ, но манипулирование любопытством по-прежнему является невероятно полезной тактикой, применяемой киберпреступниками.

«Распространение спама из вредоносных файлов JAR, которое часто приводит к появлению таких RAT, является довольно распространенным явлением. Администраторам электронной почты следует стремиться занять жесткую позицию в отношении входящих JAR-файлов и заблокировать их в своих шлюзах безопасности электронной почты», - сказала Дайана Лопера, старший исследователь безопасности в Trustwave.

Также возможно, что более продуманная электронная приманка может привести к тому, что эта QRat-кампания станет более эффективной в будущем.

«Несмотря на то, что полезная нагрузка вложения имеет некоторые улучшения по сравнению с предыдущими версиями, сама кампания по электронной почте была довольно дилетантской, и мы считаем, что вероятность того, что эта угроза будет успешно доставлена, выше, если только электронное письмо было

более сложным», - добавил Лопера». ***(Danny Palmer. This new phishing attack uses an odd lure to deliver Windows trojan malware // ZDNet (https://www.zdnet.com/article/this-new-phishing-attack-uses-an-odd-lure-to-deliver-windows-trojan-malware/). 06.01.2021).***

***

«Вредоносное программное обеспечение ElectroRAT, которое уже год в распространяется сети, начиная с 2020, и нацелено на криптокошельки обнаружено экспертом по кибербезопасности.

Исследователь из фирмы Intezer, занимающейся кибербезопасностью, выявил и задокументировал внутреннюю работу ElectroRAT, которое использовало средства жертв и истощала их.

По словам исследователя Авигайла Мехтингера, вредоносное ПО включает в себя множество подробных инструментов, обманывающих жертв, в том числе «маркетинговую кампанию, специальные приложения, связанные с криптовалютой, и новый инструмент удаленного доступа (RAT), написанный с нуля».

Вредоносное ПО называется ElectroRAT, потому что это инструмент удаленного доступа, встроенный в приложения, созданные на платформе Electron для создания приложений. Следовательно, ElectroRAT.

Что такое ElectroRAT?

Вредоносное ПО ElectroRat написано на языке программирования с открытым исходным кодом Golang, который хорошо подходит для кросс-платформенной функциональности и нацелен на несколько операционных систем, включая macOS, Linux и Windows.

Согласно отчету, в рамках операции с вредоносным ПО злоумышленники создали «регистрации доменов, веб-сайты, троянские приложения и поддельные учетные записи в социальных сетях».

В отчете Мехтингер отмечает, что, хотя злоумышленники обычно пытаются собрать закрытые ключи, используемые для доступа к кошелькам людей, обнаружить оригинальные инструменты, такие как ElectroRAT и различные приложения, написанные «с нуля», адаптированные сразу для нескольких операционных систем, довольно сложно.

«Написание вредоносного ПО с нуля также позволило кампании оставаться незамеченной в течение почти года, избегая всех обнаружений антивируса», - написал Мехтингер в своем отчете. Особенно интересно, говорит эксперт, что вредоносная программа компилируется для всех трех основных операционных систем и нацелена на них.

«Большинство вредоносных программ имеют ценность только для Windows из-за широкой базы установки и более слабой безопасности операционной системы», - говорит эксперт. «В случае с биткойном авторы вредоносных программ предполагают, что многие ранние пользователи - более технически подкованные люди, которые используют Linux».

Как это работает

Чтобы заманить жертв, злоумышленники ElectroRat создали три разных домена и приложения, работающие в нескольких операционных системах.

Страницы для загрузки приложений были созданы специально для этой операции и выглядят как легитимные объекты.

Связанные приложения специально предназначены для пользователей криптовалюты и ориентированы на них. «Jamm» и «eTrade» - приложения для управления торговлей; «DaoPoker» - это покерное приложение, в котором используется криптовалюта.

Используя поддельные соц. сети и профили пользователей, а также платя влиятельным лицам в социальных сетях за их рекламу, злоумышленник накачивал приложения, в том числе продвигал их на целевых форумах по криптовалюте и блокчейне, таких как bitcointalk и SteemCoinPan. Посты побуждали читателей смотреть на профессионально выглядящие веб-сайты и загружать приложения, хотя на самом деле они также загружали вредоносное ПО

Например, у страницы DaoPoker в Twitter было 417 подписчиков, в то время как рекламодатель в соц. сетях с более чем 25 000 подписчиков в Twitter продвигал eTrade. На момент написания статьи твиттер-страница DaoPoker все еще активна.

Хотя на первый взгляд приложения выглядят законно, они выполняют скрытые фоновые действия, нацеленные на криптовалютные кошельки пользователей. Они тоже все еще активны.

«Хакеры хотят заполучить вашу криптовалюту, и они готовы забрать все и потратить месяцы работы на создание фальшивых компаний, фальшивой репутации и невинно выглядящих приложений, которые скрывают вредоносные программы для кражи ваших сбережений», - сказал Мехтингер.

Что делает ElectroCat

«ElectroRAT имеет различные возможности, - сказал Мехтингер в электронном письме. «Он может делать снимки экрана, бекапить ключевые журналы, загружать папки/файлы с ПК жертвы и многое другое. После запуска он устанавливает команды с помощью своего командного и контрольного сервера и ждет дальнейших указаний».

В отчете предполагается, что вредоносное ПО специально нацелено на пользователей криптовалюты с целью атаки на их криптокошельки, отмечая, что жертвы комментировали сообщения, связанные с популярным приложением кошелька Ethereum Metamask. Основываясь на наблюдениях исследователей за поведением вредоносного ПО, возможно, под угрозой оказались данные более 6,5 тысяч человек.

Как этого избежать

Первый шаг - лучший, это не загружать ни одно из этих приложений.

В общем, когда вы изучаете новые приложения, исследователь советует избегать сомнительных веб-сайтов и форумов. Устанавливайте только хорошо известное и проверенное программное обеспечение; ищите приложения с длинной историей репутации и значительной базой установки.

«Не используйте кошельки, в которых хранятся закрытые ключи на вашем ноутбуке / настольном компьютере; закрытые ключи должны храниться на специальных аппаратных устройствах», - говорит эксперт.

Этот момент подчеркивает важность хранения криптовалюты в холодных аппаратных кошельках и записи исходных фраз, а не просто хранения их на вашем

компьютере. Оба эти метода делают их недоступными для вредоносных программ, которые отслеживают вашу онлайн-активность.

Есть дополнительные шаги, которые можно предпринять, если вы считаете, что ваш компьютер уже был взломан.

«Чтобы убедиться, что ваш ПК не заражен, рекомендуем предпринять активные действия и просканировать свои устройства на предмет вредоносной активности», - сказал Мехтингер.

В отчете Мехтингер предлагает, что если вы стали жертвой этого мошенничества, вам необходимо остановить запущенные процессы и удалить все файлы, связанные с вредоносным ПО. Вам также необходимо убедиться, что ваш ПК чист и на нем не запущен вредоносный код. Intezer создал Endpoint Scanner для сред Windows и Intezer Protect, бесплатный инструмент сообщества для пользователей Linux. Более подробную информацию об обнаружении можно найти в исходном отчете.

И, конечно же, следует перевести свои средства в новый криптокошелек и изменить все свои пароли.

Стремительный рост цены биткойнов привлекает больше вредоносных программ

Поскольку цена биткойнов продолжает расти, Mechtinger не видит замедления подобных атак. Фактически, они, вероятно, увеличатся.

«На кону большие капиталы, что является классикой для финансово мотивированных хакеров», - сказала она.

Эксперт заявляет, что мы увидим, как злоумышленники будут вкладывать все больше и больше ресурсов в поиск новых способовввыманивания у людей их закрытых ключей.

«Хотя для разработки новой атаки требуется гораздо больше усилий и времени, выгода также потенциально выше, потому что она с большой вероятностью обманет много людей, поскольку знания об этом стиле атаки не были распространены среди пользователей», - отметил эксперт». ***(Романов Роман. Отчёт: Вредоносное ПО с открытым исходным кодом для взлома криптокошельков обнаружено в сети // Internetua (https://internetua.com/otcset-vredonosnoe-po-s-otkrytym-ishodnym-kodom-dlia-vzloma-cryptokoshelkov-obnarujeno-v-seti). 06.01.2021).***

***

«Злоумышленники активно сканируют Интернет на предмет открытых SSH-устройств и пытаются войти в них, используя новый, недавно исправленный, бэкдор с жестко заданными учетными данными Zyxel.

В прошлом месяце Нильс Тьюзинк из голландской фирмы EYE, занимающейся кибербезопасностью, раскрыл секретную жестко закодированную учетную запись бэкдора в брандмауэрах Zyxel и контроллерах AP. Эта секретная учетная запись «zyfwp» позволяла пользователям входить в систему через SSH и веб-интерфейс, чтобы получить права администратора.

В сообщении Zyxel заявляет, что они использовали секретную учетную запись для автоматической доставки обновлений прошивки через FTP.

Этот бэкдор представляет собой значительный риск, поскольку он может позволить злоумышленникам создавать учетные записи VPN для доступа к внутренним сетям или перенаправлять внутренние службы, чтобы сделать их доступными для удаленного доступа и использовать их.

Злоумышленники активно ищут бэкдор Zyxel

Вчера компания GreyNoise, занимающаяся разведкой кибербезопасности, обнаружила три разных IP-адреса, которые активно сканируют устройства SSH и пытаются войти в них, используя учетные данные Zyxel backdoor.

Генеральный директор GreyNoise Эндрю Моррис сказал BleepingComputer, что злоумышленник, похоже, не сканирует специально устройства Zyxel, а вместо этого сканирует Интернет в поисках IP-адресов, на которых работает SSH.

Когда SSH обнаружен, он попытается подобрать учетную запись на устройстве, при этом одна из проверенных учетных данных будет новой учетной записью Zyxel 'zyfwp' backdoor.

Особый интерес представляет то, что один из IP-адресов использует встроенный SSH-клиент Cobalt Strike для выполнения сканирования. Моррис сказал BleepingComputer, что злоумышленник может сканировать таким образом, чтобы избежать поставщиков информации об угрозах.

В прошлом месяце Zyxel выпустил «ZLD V4.60 Patch 1», который удаляет бэкдор-аккаунты на брандмауэрах. Вчера Zyxel объявил, что выпустит патч для контроллеров AP 8 января 2021 года.

BleepingComputer настоятельно рекомендует всем пользователям как можно скорее установить патч, чтобы предотвратить получение злоумышленниками доступа к уязвимым сетям, развертывания программ-вымогателей или кражи данных». ***(Lawrence Abrams. Hackers start exploiting the new backdoor in Zyxel devices // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-start-exploiting-the-new-backdoor-in-zyxel-devices/). 06.01.2021).***

***

«Исследователи из Recorded Future сообщают о росте числа взломанных Cobalt Strike и других состязательных инструментов с открытым исходным кодом и простыми в использовании интерфейсами.

По словам исследователей, простые в использовании и развертывании агрессивные инструменты безопасности, упрощающие, чем когда-либо, для преступников, не обладающих техническими знаниями, вмешательство в киберпреступность, наблюдается значительный рост.

Recorded Future только что опубликовал результаты своих регулярных наблюдений за вредоносной инфраструктурой в конце года, выявив более 10 000 уникальных серверов управления и контроля (C2) для 80 семейств вредоносных программ, почти все из которых связаны с группами расширенных постоянных угроз (APT) или «высокопроизводительными» финансовые деятели».

В отчете Recorded Future о противоборствующей инфраструктуре за 2020 год поясняется, что исследователи ожидают более широкого внедрения инструментов с

открытым исходным кодом, поскольку они просты в использовании и доступны злоумышленникам без глубоких технических знаний.

«В следующем году Recorded Future ожидает дальнейшего внедрения инструментов с открытым исходным кодом, которые недавно приобрели популярность, в частности Covenant, Octopus C2, Sliver и Mythic», - говорится в отчете. «Три из этих инструментов имеют графический пользовательский интерфейс, что упрощает их использование для менее опытных операторов, и все четыре имеют подробную документацию по их использованию».

Открытый исходный код и Cobalt Strike доминируют

Исследователи продолжают объяснять, что с момента утечки исходного кода Cobalt Strike в ноябре прошлого года на GitHub его использование увеличилось, а взломанные или пробные версии в основном использовались известными APT, включая APT41, Mustang Panda, Ocean Lotus и FIN7. В отчете говорится, что Cobalt Strike также был связан с наибольшим количеством наблюдаемых серверов C2 в прошлом году.

Cobalt Strike - это коммерчески доступный инструмент для тестирования на проникновение. Он отправляет маяки для обнаружения сетевых уязвимостей. При использовании по прямому назначению имитирует атаку. С тех пор злоумышленники выяснили, как использовать его против сетей для эксфильтрации данных, доставки вредоносного ПО и создания поддельных профилей C2, которые выглядят законными и избегают обнаружения.

Согласно Recorded Future, Cobalt Strike использовался с 1441 наблюдаемым сервером C2 в 2020 году, за ним следуют Metasploit с 1122 и PupyRat с 454.

«В наиболее часто наблюдаемых семьях преобладали инструменты с открытым исходным кодом или коммерчески доступные инструменты», - говорится в отчете. «Обнаружения неизмененных развертываний Cobalt Strike (предварительно настроенный сертификат TLS, порт администрирования Team Server или контрольные заголовки HTTP) составили 13,5% от общего числа идентифицированных серверов C2. Metasploit и PupyRAT представляли другие ведущие серверы управления и контроля с открытым исходным кодом, определенные Recorded Future».

Ссылки на APT

В отчете добавлено, что почти все наблюдаемые средства безопасности (OST), включая Cobalt Strike и другие, можно проследить до атак со стороны APT-участников.

«Почти все OST, обнаруженные Recorded Future, связаны с APT или высококлассными финансовыми субъектами», - говорится в отчете. «Простота доступа и использования этих инструментов в сочетании с неясностью потенциальной атрибуции делает их привлекательными как для несанкционированных вторжений, так и для красных команд».

Согласно отчету Kaspersky о тенденциях в области APT за 2020 год, общий ландшафт APT-угроз за последний год стал более сложным благодаря широко распространенным инновациям в группах APT с различными тактиками, методами и процедурами (TTP).

Как только исследователи смогли идентифицировать серверы C2, они отследили их до 576 различных хостинг-провайдеров. Больше всего размещено на Amazon - 471, или около 3,8 процента. Другой ведущий из США, Digital Ocean, занял второе место в списке с 421. В отчете поясняется, что это не обязательно красный флаг.

«Развертывание контроллеров Cobalt Strike и Metasploit на этих провайдерах не свидетельствует о злоупотреблении служебным положением или небрежном хостинге, но более вероятно из-за того, что уполномоченные красные группы используют эти инструменты в облачной инфраструктуре», - говорится в отчете.

Recorded Future объяснила, что цель этого постоянного аудита вредоносной инфраструктуры состоит в том, чтобы помочь командам безопасности идентифицировать действующих лиц в процессе их настройки, а не ждать, пока они начнут работать и смогут нанести удар. Отчет показал, что у команд есть 61-дневное время выполнения заказа с момента создания сервера C2 до момента его обнаружения. В отчете добавлено, что среднее время, в течение которого на этих серверах размещается вредоносная инфраструктура, составляет 54,8 дня.

Но обнаружение до того, как вредоносная инфраструктура может быть использована, дает возможность остановить злоумышленников до того, как они нанесут ущерб, согласно Recorded Future.

«Прежде чем сервер может быть использован злоумышленником, он должен быть приобретен путем компрометации или законной покупки», - поясняет Recorded Future. «Затем необходимо установить программное обеспечение, настроить конфигурации и добавить файлы на сервер. Акторы должны получить к нему доступ через вход в панель, протоколы SSH или RDP, а затем выставить контроллер вредоносного ПО через порт, чтобы данные могли передаваться от жертвы и управлять командами для заражения. Только тогда сервер можно будет использовать в злонамеренных целях». ***(Becky Bracken. Malicious Software Infrastructure Easier to Get and Deploy Than Ever // Threatpost (https://threatpost.com/malicious-software-infrastructure-easier-deploy/162913/). 08.01.2021).***

***

«Более пяти лет пользователи macOS были объектами скрытой вредоносной операции, которая использовала хитрый трюк, чтобы избежать обнаружения, и захватывала аппаратные ресурсы зараженных пользователей для добычи криптовалюты за их спиной.

Названный OSAMiner, вредоносная программа была распространена в дикой природе, по крайней мере, к 2015 году под видом пиратской (крекинг) игр и программного обеспечения, таких как Лига Легенд и Microsoft Office для Mac, безопасности фирмы SentinelOne говорится в докладе, опубликованном на этой неделе.

«OSAMiner был активен в течение долгого времени и в последние месяцы развился», - сказал ZDNet в понедельник в интервью ZDNet представитель SentinelOne.

«Судя по имеющимся у нас данным, он в основном нацелен на общины китайцев / жителей Азиатско-Тихоокеанского региона», - добавил представитель.

ВЛОЖЕННЫЕ СЦЕНАРИИ APPLESCRIPTS, ПРЕДНАЗНАЧЕННЫЕ ТОЛЬКО ДЛЯ ВЫПОЛНЕНИЯ, ДЛЯ ПОБЕДЫ!

Но криптомайнер не остался незамеченным. SentinelOne сообщил, что две китайские охранные фирмы обнаружили и проанализировали более старые версии OSAMiner в августе и сентябре 2018 года соответственно.

Но их отчеты лишь поверхностно описывают то, на что способен OSAMiner, сказал вчера Фил Стоукс, исследователь вредоносного ПО для macOS из SentinelOne.

Основная причина заключалась в том, что исследователи безопасности не могли получить весь код вредоносной программы в то время, которая использовала вложенные файлы AppleScript, предназначенные только для выполнения, для извлечения своего вредоносного кода на разных этапах.

По мере того, как пользователи устанавливали пиратское программное обеспечение, установщики с ловушками загружали и запускали AppleScript только для выполнения, который загружал и запускал второй AppleScript, предназначенный только для выполнения, а затем еще один, последний, третий AppleScript, предназначенный только для выполнения.

Поскольку AppleScript «только для выполнения» находится в скомпилированном состоянии, в котором исходный код не читается человеком, это усложняет анализ для исследователей безопасности.

Вчера Стоукс опубликовал полную цепочку этой атаки вместе с индикаторами компрометации (IOC) прошлых и новых кампаний OSAMiner. Стоукс и команда SentinelOne надеются, что, наконец, раскрыв тайну, окружающую эту кампанию, и опубликовав IOC, другие поставщики программного обеспечения для обеспечения безопасности macOS теперь смогут обнаруживать атаки OSAMiner и защищать пользователей macOS.

«Только запускаемые сценарии AppleScripts на удивление редки в мире вредоносных программ для macOS, но и долговечность, и отсутствие внимания к macOS. Кампания OSAMiner, которая, вероятно, длится не менее 5 лет, показывает, насколько эффективны только запускаемые сценарии Apple может быть для уклонения и антианализа», - заключил вчера Стоукс в своем докладе.

«В этом случае мы не видели, чтобы субъект использовал какие-либо более мощные функции AppleScript, которые мы обсуждали в другом месте [1, 2], но это вектор атаки, который остается широко открытым и которым многие защитные инструменты не оснащены. обрабатывать.» ***(Catalin Cimpanu. macOS malware used run-only AppleScripts to avoid detection for five years // ZDNet (https://www.zdnet.com/article/macos-malware-used-run-only-applescripts-to-avoid-detection-for-five-years/). 12.01.2021).***

***

«Веб-оболочка BumbleBee позволяет злоумышленникам APT загружать и скачивать файлы, а также перемещаться по сторонам, выполняя команды.

Веб-оболочка под названием BumbleBee приняла участие в продолжающейся шпионской кампании xHunt, нацеленной на серверы Microsoft Exchange в кувейтских организациях.

По словам исследователей из подразделения 42 Palo Alto Networks, еще в сентябре BumbleBee (названный так из-за своей цветовой схемы) использовался для загрузки и выгрузки файлов на и с взломанного сервера Exchange.

«Мы обнаружили, что BumbleBee размещен на внутреннем веб-сервере Internet Information Services (IIS) в той же сети, что и взломанный сервер Exchange, а также на двух внутренних веб-серверах IIS в двух других кувейтских организациях», - пояснили исследователи в блоге в понедельник.

Анализ показал, что злоумышленники использовали VPN-доступ для прямого разговора с BumbleBee, часто переключаясь между разными VPN-серверами, которые оказались из разных стран, включая Бельгию, Германию, Ирландию, Италию, Люксембург, Нидерланды, Польшу, Португалию, Швецию и США. Царство.

Как выяснила компания, этот смешанный подход также подтвердился при смене различных операционных систем и браузеров, в частности, Mozilla Firefox или Google Chrome в системах Windows 10, Windows 8.1 или Linux.

«Мы считаем, что это попытка избежать обнаружения и затруднить анализ вредоносных действий», - отмечают исследователи Unit 42. «Это [также] предполагает, что субъект имеет доступ к нескольким системам и использует его, чтобы усложнить анализ действий, или что в нем участвуют несколько субъектов, которые имеют разные предпочтения в отношении операционных систем и браузеров».

BumbleBee также использовался для бокового перемещения, выполняя команды злоумышленников для обнаружения дополнительных систем. И действительно, исследователи обнаружили дополнительные веб-оболочки BumbleBee, размещенные на внутренних веб-серверах IIS, которые не подключены к Интернету ни у одной из трех кувейтских организаций. Для взаимодействия с ними кибератаки использовали туннели SSH, созданные с помощью инструмента PuTTY Link (Plink).

«Мы наблюдали, как субъект использует Plink для создания SSH-туннеля для TCP-порта 3389, что предполагает, что субъект использовал туннель для доступа к системе с использованием протокола удаленного рабочего стола (RDP)», - пишут исследователи. «Мы также наблюдали, как субъект создает туннели SSH для внутренних серверов для TCP-порта 80, что предполагает, что субъект использовал туннель для доступа к внутренним веб-серверам IIS. Мы полагаем, что субъект получил доступ к этим дополнительным внутренним веб-серверам IIS, чтобы использовать функцию загрузки файлов во внутренних веб-приложениях, чтобы установить BumbleBee в качестве метода бокового перемещения».

BumbleBee: запрос пароля

Изучив веб-оболочку глубже, Unit 42 обнаружил, что BumbleBee требует от злоумышленника предоставить один пароль для просмотра веб-оболочки и второй пароль для взаимодействия с ней.

«Актер должен [сначала] предоставить пароль в параметре URL с именем параметр», - заявляет компания. «В противном случае форма, используемая для взаимодействия с BumbleBee, не будет отображаться в браузере. Чтобы проверить предоставленный пароль для аутентификации, веб-оболочка сгенерирует хэш MD5 значения параметра и проверит его с помощью жестко запрограммированного хеша MD5».

Как только операторы получают доступ к BumbleBee, он предоставляет три основных функции: выполнение команд, а также загрузка и скачивание файлов с взломанного сервера.

«Чтобы выполнить любую из этих функций, актер должен предоставить второй пароль», - пишут исследователи. «Веб-оболочка BumbleBee сгенерирует хеш-код пароля MD5 и проверит его с помощью жестко запрограммированного хеш-кода MD5 перед выполнением этой функции».

BumbleBee: Шмель-шпион

Просматривая журналы сервера IIS и другие журналы с сервера Exchange, исследователи могли наблюдать запросы HTTP POST, генерируемые, когда злоумышленники отправляли команды через BumbleBee.

После некоторого дополнительного анализа исследователи смогли составить более полную картину того, для чего конкретно используется BumbleBee.

«16 сентября 2020 г. актер провел три часа 37 минут, выполняя команды через веб-оболочку BumbleBee, установленную на [первом] скомпрометированном сервере Exchange», - говорится в анализе.

Действия включали обнаружение сети с использованием команд ping и net group, а также PowerShell для поиска дополнительных компьютеров в сети; и выполнение обнаружения учетной записи с помощью команд whoami и quser. Также злоумышленники определяли системное время с помощью команд W32tm и time; и создал туннель SSH с помощью Plink к удаленному хосту и использовал RDP через этот туннель SSH для управления скомпрометированным компьютером. Они также выполнили боковое перемещение к другой системе, установив общую папку; и, наконец, они удалили доказательства атаки, удалив BumbleBee после того, как они закончили отдавать команды.

Помимо анализа команд, выполняемых на скомпрометированном сервере Exchange, Unit 42 также анализировал команды, выполняемые в веб-оболочке BumbleBee на внутреннем веб-сервере IIS, размещенном в одной из двух других кувейтских организаций.

«10 сентября 2020 года мы обнаружили, что актер выполнил несколько команд для обнаружения сети и учетных записей пользователей. Кроме того, актер использовал BumbleBee для загрузки второй веб-оболочки с именем файла cq.aspx. Актер использовал эту вторую веб-оболочку для запуска сценария PowerShell, который отправлял SQL-запросы к базе данных Microsoft SQL Server».

Текущая кампания

Известная xHunt группа угроз, которая впервые была обнаружена в 2018 году и ранее запущен целый ряд атак, нацеленных на правительство Кувейта, а также судоходных и транспортных организаций, постоянно обновляется арсенал инструментов, все в службе шпионить их цели.

Самая последняя кампания длилась до февраля, когда xHunt взломал сервер Exchange через Outlook Web App, используя скомпрометированные учетные данные.

«Актер использовал функцию поиска в Outlook Web App для поиска адресов электронной почты, включая поиск доменного имени скомпрометированной кувейтской организации, чтобы получить полный список адресов электронной почты, а также определенные ключевые слова, такие как служба поддержки», - пояснили исследователи. «Мы также видели, как актер просматривал электронные письма в почтовом ящике скомпрометированной учетной записи, в частности электронные письма от поставщиков услуг и поставщиков технологий. Кроме того, актер просматривал электронные письма с предупреждениями от продуктов Symantec и Fortinet FortiWeb».

Этот поиск электронных писем в службу поддержки и просмотр электронных писем с предупреждениями безопасности предполагает, что xHunt держал в курсе, заметила ли кувейтская организация вредоносную активность.

«Попытки скрыть свое местонахождение и сосредоточение внимания на просмотре электронных писем, которые могут уведомить администраторов скомпрометированной сети о присутствии злоумышленника, могут объяснить, как злоумышленник смог поддерживать присутствие в скомпрометированной сети в течение многих месяцев», - отметили исследователи». ***(Tara Seals. BumbleBee Opens Exchange Servers in xHunt Spy Campaign // Threatpost (https://threatpost.com/bumblebee-exchange-servers-xhunt-spy/162973/). 12.01.2021).***

***

«В этом месяце исследователь безопасности запустил веб-портал, на котором перечислены уязвимости в коде распространенных вредоносных программ. Исследователь надеется, что другие специалисты по безопасности будут использовать ошибки для сбоя, отключения и удаления вредоносных программ на зараженных хостах в рамках операций реагирования на инциденты.

Новый портал MalVuln, созданный и запущенный охотником за ошибками Джоном Пейджем, доступен на сайте malvuln.com.

Сам сайт - это типичный портал для выявления уязвимостей. В нем перечисляется название программного обеспечения (в данном случае название вредоносной программы), технически подробно описывается уязвимость и приводится код эксплойта для подтверждения концепции (PoC), чтобы другие могли воспроизвести проблему.

Пейдж рассказал ZDNet, что создал сайт от скуки во время недавней блокировки COVID-19.

«Это выходит за рамки нормы, никогда не было специального веб-сайта для такого рода вещей», - сказал исследователь ZDNet в интервью по электронной почте.

В настоящее время MalVuln насчитывает 45 недостатков безопасности. Некоторые из них предназначены для текущих угроз, таких как Phorpiex (Trik), но также и для старых вредоносных программ, таких как Bayrob.

Пейдж сказал, что все уязвимости, перечисленные на MalVuln на данный момент, принадлежат ему.

«Посторонних заявок не поступало, и в настоящее время я их не принимаю», - сказал Пейдж. Тем не менее, ключ PGP указан на сайте, и мы планируем разрешить другим присылать свои результаты когда-нибудь в будущем.

СПОРЫ НАЗРЕВАЮТ?

Но сайт также затрагивает деликатную тему в сфере кибербезопасности. На протяжении десятилетий исследователи безопасности тайно взламывали против операторов вредоносных программ.

Подобно тому, как вредоносное ПО иногда использует ошибки в законных приложениях для проникновения в системы, охранные фирмы также используют ошибки в коде вредоносного ПО для проникновения в инфраструктуру злоумышленника.

Охранные фирмы часто взламывают командный сервер вредоносного ПО, чтобы получить данные о жертвах, или используют ошибки в вредоносном ПО, чтобы отключить и удалить его из зараженных систем.

Эта практика была тщательно охраняемым секретом, в первую очередь из-за юридических последствий, связанных с практикой «обратного взлома», и преимуществ, которые дает тайное злоупотребление ошибками вредоносных программ для отслеживания злоумышленников.

Например, в течение многих лет охранная компания Fox-IT использовала ошибку в Cobalt Strike, законном инструменте, которым злоупотребляют банды киберпреступников, для отслеживания местоположения возможных серверов управления и контроля вредоносного ПО. Компания сообщила, что сделала это только после того, как в 2019 году была обнаружена и исправлена ошибка.

Поэтому неудивительно, что когда в начале этого месяца был запущен такой веб-сайт, как MalVuln, было немало ворчаний о том, как MalVuln раздавал эти тщательно охраняемые секреты и косвенно помогал операторам вредоносных программ, указывая на ошибки в их коде, эффективно убирая ценные инструменты от охранных фирм и служб реагирования на инциденты.

Но Пейдж сказал ZDNet, что его не волнует этот аспект.

«Я занимаюсь своим делом и не отвечаю. Обычно это те же люди, которые думают, что уязвимости не должны публиковаться, потому что это помогает злоумышленникам», - сказал он.

И Пейдж не единственный, кто разделяет это мнение, поскольку другие исследователи в области безопасности требуют большей открытости в отношении этой практики и большего обмена такими деталями в сообществе кибербезопасности.

В любом случае, тема будет оставаться спорной, но MalVuln затронул реальный вопрос - что вредоносные программы также содержат ошибки, так же, как обычное программное обеспечение.

«Существует множество вредоносных программ, ненавидящих себя», - сказал Пейдж, пообещав выпускать больше вредоносных программ в будущем». ***(Catalin Cimpanu. New website launched to document vulnerabilities in malware strains //***

ZDNet (https://www.zdnet.com/article/new-website-launched-to-document-vulnerabilities-in-malware-strains/). 22.01.2021).

***

«Инструмент обнаружения-уклонения, libprocesshider, скрывает вредоносное ПО TeamTNT от программ обработки информации.

Группа угроз TeamTNT добавила в свой арсенал новый инструмент для обнаружения и уклонения, помогающий группам защиты обходить вредоносное ПО, занимающееся криптодобычей.

Группа киберпреступности Тимтнта известна облачные атаки, включая нацеливание учетных данные Amazon Web Services (AWS), чтобы ворваться в облако, и использовать его в шахту для криптовалюта Monero. Он также ранее был нацелен на облачные экземпляры Docker и Kubernetes.

Новый инструмент обнаружения и уклонения, libprocesshider, скопирован из репозиториев с открытым исходным кодом. Инструмент с открытым исходным кодом с 2014 года находится на Github и описывается как имеющий возможность «скрыть процесс в Linux с помощью предзагрузчика ld».

«Хотя новая функциональность libprocesshider заключается в том, чтобы избежать обнаружения и других основных функций, она действует как индикатор, который следует учитывать при поиске вредоносной активности на уровне хоста», - заявили исследователи из Alien Labs AT&T в среду.

Новый инструмент поставляется в виде сценария в кодировке base64, скрытого в двоичном файле криптомайнера TeamTNT, или через его бот Internet Relay Chat (IRC), называемый TNTbotinger, который способен к распределенным атакам типа «отказ в обслуживании» (DDoS).

«Я нашел несколько файлов TeamTNT на VirusTotal с помощью этого инструмента, и есть большая вероятность, что они были загружены зараженными пользователями, а не кем-либо, имеющим отношение к TeamTNT, поэтому я считаю, что ... он используется в дикой природе», - Офер Каспи, Об этом Threatpost сообщил исследователь безопасности AT&T Alien Labs.

В цепочке атаки после загрузки сценария в кодировке base64 он выполняет несколько задач. К ним относятся изменение сетевой конфигурации DNS, установка постоянства (через systemd), загрузка последней конфигурации IRC-бота, очистка свидетельств активности - и удаление и активация libprocesshider. Инструмент удаляется как скрытый файл архива на магнитной ленте (также известный как формат Tar, который используется для распространения программного обеспечения с открытым исходным кодом) на диске, а затем распаковывается сценарием и записывается в '/ usr / local / lib / systemhealt. так'.

Затем libprocesshider стремится скрыть вредоносный процесс от программ обработки информации, таких как `ps 'и` lsof'.

Это оба средства просмотра процессов, которые используют файл / usr / bin / sbin. Программа 'ps' (сокращение от «статус процесса») отображает текущие процессы во многих Unix-подобных операционных системах; Между тем, lsof - это команда (сокращение от «list open files»), также используемая в Unix-подобных операционных системах, чтобы, как следует из названия, сообщить список всех

открытых файлов и процессов, которые их открыли. Скрытие процесса от этих двух инструментов просмотра процессов позволит злоумышленнику скрыть свою вредоносную деятельность.

libprocesshider использует процесс, называемый предварительной загрузкой, чтобы скрыть свою активность от ps и lsof. Этот процесс позволяет системе загружать настраиваемую общую библиотеку до загрузки других системных библиотек.

«Если пользовательская разделяемая библиотека экспортирует функцию с такой же сигнатурой, что и функция, находящаяся в системных библиотеках, пользовательская версия переопределит ее», - говорят исследователи.

Затем загруженная пользовательская разделяемая библиотека позволяет инструменту реализовать функцию readdir (). Эта функция используется такими процессами, как `ps 'для чтения каталога / proc и поиска запущенных процессов. Он использует эту функцию для изменения возвращаемого значения на случай, если ps обнаружит вредоносный процесс, чтобы скрыть его.

TeamTNT продолжает добавлять новые функции

Время от времени было замечено, что TeamTNT развертывает различные обновления для своего вредоносного ПО для криптомайнинга, включая новый загрузчик памяти, обнаруженный всего несколько недель назад, который был основан на Ezuri и написан на GOlang.

В августе был обнаружен червь-майнер TeamTNT, распространяющийся через облако AWS и собирающий учетные данные. Затем, после перерыва, группа TeamTNT вернулась в сентябре, чтобы атаковать облачные экземпляры Docker и Kubernetes, злоупотребляя законным инструментом облачного мониторинга под названием Weave Scope». ***(Lindsey O'Donnell. TeamTNT Cloaks Malware With Open-Source Tool // Threatpost (https://threatpost.com/teamtnt-cloaks-malware-open-source-tool/163414/). 27.01.2021).***

***

«Новая версия NAT slipstreaming позволяет киберпреступникам легко добраться до устройств, не подключенных к Интернету.

Отключение устройств от Интернета больше не является надежным планом защиты их от удаленных злоумышленников. Обнаружена новая версия известной атаки с трансляцией сетевых адресов (NAT), которая позволяет удаленным злоумышленникам достигать нескольких внутренних сетевых устройств, даже если эти устройства не имеют доступа к Интернету.

По словам исследователей из Армиса и Сами Камкара, главного сотрудника службы безопасности и соучредителя Openpath Security, злоумышленники могут выполнить атаку, просто убедив одну цель, имеющую доступ к Интернету в сети, перейти по вредоносной ссылке. Оттуда киберпреступники могут получить доступ к другим, незащищенным конечным точкам, включая неуправляемые устройства, такие как промышленные контроллеры, без дополнительной социальной инженерии.

NAT - это процесс подключения внутренних сетевых устройств к внешнему Интернету; по сути, это позволяет маршрутизатору безопасно разрешать

нескольким подключенным к нему устройствам совместно использовать один общедоступный IP-адрес. В корпоративных средах функции NAT сочетаются с межсетевыми экранами, чтобы обеспечить лучшую кибербезопасность периметра; все продукты Fortinet, Cisco и HPE используют этот подход.

Обзор NAT Slipstreaming

В исходной атаке NAT slipstreaming, выявленной и смягченной в ноябре, злоумышленник убеждает жертву посетить специально созданный веб-сайт (с помощью социальной инженерии и других методов); жертва во внутренней сети, которая нажимает на нее, затем попадает на сайт злоумышленника. Веб-сайт, в свою очередь, обманывает NAT сети жертвы, открывая входящий путь (порта TCP или UDP) из Интернета к устройству жертвы.

«Скользящий поток легко использовать, поскольку он, по сути, полностью автоматизирован, работает как в разных браузерах, так и в платформах, и не требует какого-либо взаимодействия с пользователем, кроме посещения сайта жертвы», - сказал Камкар Threatpost прошлой осенью.

Для запуска атаки на устройстве жертвы также должен быть включен механизм отслеживания соединений на уровне приложений (ALG), который обычно встроен в NAT. NAT slipstreaming использует браузер пользователя вместе с ALG.

«Эта атака использует преимущество произвольного управления частью данных некоторых пакетов TCP и UDP без включения HTTP или других заголовков; атака использует эту новую технику внедрения пакетов во всех основных современных (и старых) браузерах», - пояснил Камкар.

При атаке, когда устройство жертвы посещает веб-сайт, контролируемый злоумышленником, код JavaScript, выполняемый в браузере жертвы, отправляет дополнительный трафик на сервер злоумышленника, который проходит через сетевой NAT / брандмауэр.

«Этот трафик второй фазы формируется таким образом, что NAT обманывается, полагая, что этот трафик действительно исходит от приложения, которое требует второго подключения, от Интернета к устройству жертвы и к внутреннему порту, который злоумышленник может выбирать», - пояснили исследователи. «Это второе соединение может привести к тому, что злоумышленник получит доступ к любой службе (TCP / UDP) на устройстве жертвы прямо из Интернета».

Если, например, устройство жертвы является устройством Windows, уязвимым для EternalBlue, злоумышленник может получить доступ к порту SMB на устройстве жертвы, используя этот метод, из Интернета, воспользоваться уязвимостью и захватить устройство.

«Единственное, что требуется для проведения этой атаки, - это то, что жертва нажимает на ссылку или посещает веб-страницу, в которую злоумышленник внедрил некоторый код JavaScript», - отметили исследователи.

NAT Slipstreaming 2.0

По словам исследователей, только что открытый вариант подхода просто расширяет возможности атаки.

Теперь «злоумышленники [могут] обмануть NAT таким образом, чтобы он создавал входящие пути к любому устройству во внутренней сети, а не только к устройству жертвы, которое щелкнуло по ссылке», - пояснили они в публикации блога на Вторник.

Проблема заключается в H.323 ALG, где он поддерживается. В отличие от большинства других ALG, H.323 позволяет злоумышленнику создать отверстие в NAT / брандмауэре для любого внутреннего IP-адреса, а не только для IP-адреса жертвы, которая нажимает на вредоносную ссылку.

Между тем, соединения WebRTC TURN могут быть установлены браузерами через TCP на любой порт назначения. Список ограниченных портов браузеров не использовался этой логикой и поэтому был пропущен.

«Это позволяет злоумышленнику достигать дополнительных ALG, таких как FTP и IRC ALG (порты 21, 6667), которые ранее были недоступны из-за списка ограниченных портов», - говорят исследователи. «FTP ALG широко используется в NAT / межсетевых экранах»…

Возможность доступа к устройствам без вмешательства человека означает, что злоумышленники могут достичь не только настольных компьютеров, но и других устройств, которые обычно не имеют оператора - неуправляемых устройств, таких как принтеры, промышленные контроллеры, аксессуары Bluetooth, IP-камеры, датчики, интеллектуальное освещение и многое другое. Исследователи отметили, что воздействие на них может быть серьезным - от отказа в обслуживании (DoS) до полномасштабной атаки с использованием программ-вымогателей.

Неуправляемые корпоративные устройства в опасности

«Неуправляемые устройства [часто] не обладают встроенными возможностями безопасности и часто предлагают интерфейсы для управления ими и доступа к их данным с минимальной аутентификацией во внутренней сети», - пояснили исследователи. «Открытие доступа к этим интерфейсам напрямую через Интернет - серьезная угроза безопасности».

Исследователи привели пример офисного принтера, которым можно управлять через стандартный протокол печати или через внутренний веб-сервер. Используя NAT slipstreaming, злоумышленник может отключить его или заставить распечатать произвольные документы. В зависимости от функций принтера киберпреступники также могут получить доступ к сохраненным документам.

Исследователи добавили, что для выполнения таких действий новый открытый интерфейс должен быть небезопасным, как и другие цели. Таким образом, как только злоумышленники создают веб-соединение с целью, им необходимо получить доступ к этой цели. Исследователи отметили, что многие неуправляемые устройства, не подключенные к Интернету, не требуют паролей или часто остаются без исправлений.

«Помимо интерфейсов, не прошедших аутентификацию по своей конструкции, многие неуправляемые устройства также могут быть уязвимы для широко известных уязвимостей, которыми можно воспользоваться, если злоумышленник сможет обойти NAT / брандмауэр и инициировать сетевой трафик, который может их запустить, " они написали.

Примером этого риска являются 97 процентов промышленных контроллеров, которые, как недавно было установлено, остаются уязвимыми для группы СРОЧНЫХ / 11 ошибок безопасности. Исследователи объяснили, что во многих промышленных сценариях регулярное исправление неуправляемых устройств является проблемой, поскольку их часто невозможно отключить из-за производственных требований. Таким образом, «многие организации полагаются на защиту периметра (брандмауэры и NAT), чтобы защитить свои непропатченные устройства от доступа потенциальных злоумышленников в Интернете».

Как только периметр нарушен, злоумышленники могут использовать уязвимые и открытые устройства, захватывать их и устанавливать инструменты удаленного доступа для дальнейших атак.

Смягчение с помощью исправления браузера

Как и исходная атака, новая версия была смягчена с помощью патчей для браузеров Chrome, Safari, Firefox и Edge. Chromium отслеживает новый вариант через CVE-2020-16043, а Firefox отслеживает его через CVE-2021-23961.

«В то время как основная проблема этой атаки заключается в том, как реализованы NAT (различными способами в маршрутизаторах и межсетевых экранах, у многих поставщиков и приложений), самый простой и быстрый способ смягчить последствия - это установить патч для браузеров», - говорится в сообщении.

Обновления - это Chrome v87.0.4280.141, Firefox v85.0 и Safari v14.0.3, а браузер Microsoft Edge теперь также исправлен, поскольку он основан на исходном коде Chromium». ***(Tara Seals. Remote Attackers Can Now Reach Protected Network Devices via NAT Slipstreaming // Threatpost (https://threatpost.com/remote-attackers-internal-network-devices-nat-slipstreaming/163400/). 27.01.2021).***

***

«Сложный и опасный, DanaBot снова появился после семи месяцев бездействия.

Исследователи предупреждают, что новая четвертая версия банковского трояна DanaBot появилась после месяцев загадочного затишья. Последний вариант, который все еще анализируется исследователями, вызывает опасения, учитывая количество прошлых эффективных кампаний DanaBot.

По данным Proofpoint, с мая 2018 года по июнь 2020 года DanaBot был неотъемлемой частью ландшафта угроз преступного ПО, который впервые обнаружил вредоносное ПО в 2018 году и опубликовал во вторник отчет о последнем варианте.

«Начиная с конца октября 2020 года, мы наблюдали значительное обновление образцов DanaBot, появившихся в VirusTotal», - написали Деннис Шварц, Аксель Ф. и Брэндон Мерфи в совместном отчете во вторник. «Хотя он не вернулся к своему прежнему масштабу, DanaBot - это вредоносная программа, которую защитники должны снова обратить на себя».

ДанаБот Деструктор

DanaBot - это банковский троян, который сначала нацелился на пользователей в Австралии через электронные письма, содержащие вредоносные

URL-адреса. Затем преступники разработали второй вариант и нацелены на компании США - часть серии крупномасштабных кампаний. Третий вариант появился в феврале 2019 года, который был значительно расширен за счет функции удаленного управления и контроля, по словам исследователей ESET, которые его обнаружили.

Хотя последняя четвертая версия, найденная Proofpoint, уникальна, из недавнего отчета исследователя неясно, какие именно новые возможности, если таковые имеются, есть у вредоносного ПО сегодня. Proofpoint не ответил на запросы прессы.

По сравнению с предыдущими кампаниями, отчет вторника предполагает, что этот последний вариант снабжен в основном тем же смертоносным арсеналом инструментов, что и раньше. Основные функции включают компонент ToR для анонимности связи между злоумышленниками и зараженным оборудованием.

«Как ранее сообщалось в панели управления DanaBot, мы считаем, что DanaBot настроен как« вредоносная программа как услуга », в которой один злоумышленник контролирует глобальную панель управления и контроля (C&C), а инфраструктура затем продает доступ другим участникам угроз, известным как филиалы», - пишут исследователи.

В ядре DanaBot

В общем, многоступенчатая цепочка заражения DanaBot начинается с капельницы, запускающей каскадное развитие взломов. К ним относятся кража сетевых запросов, перекачивание учетных данных приложений и служб, кража конфиденциальной информации, заражение программами-вымогателями, слежение за скриншотами рабочего стола и удаление криптомайнера для превращения целевых компьютеров в рабочих криптовалюты.

В своем текущем анализе Proofpoint сосредоточился на конкретных технических изменениях в «Основном компоненте» вредоносной программы. Этот аспект вредоносного ПО включал функции антианализа, а также:

Некоторые функции Windows API разрешаются во время выполнения.

Когда файл, связанный с вредоносным ПО, читается или записывается в файловую систему, это выполняется в процессе чтения или записи безопасного файла-обмана.

Постоянство поддерживается путем создания файла LNK, который выполняет основной компонент в каталоге запуска пользователя.

Файлы LNK (или файлы ярлыков Windows) - это файлы, автоматически создаваемые Windows, когда пользователь открывает их файлы. Эти файлы используются Windows для подключения типа файла к определенному приложению, используемому для просмотра или редактирования цифрового контента.

Обнаружены дополнительные обновления

В этом новом варианте исследователи определили несколько новых идентификаторов партнеров, предполагая, что компонент «вредоносное ПО как услуга» для DanaBot был очень активен и продолжал расти. Также были отмечены новые тактики и методы заражения.

«Исследователи Proofpoint смогли сузить по крайней мере один из методов распространения DanaBot до различных программных продуктов и сайтов взлома, которые якобы предлагают программные ключи и взломы для бесплатной загрузки, включая антивирусные программы, VPN, графические редакторы, редакторы документов и игры», - пишут исследователи.

Незаконный контент или программные инструменты, загруженные с этих сайтов, определяются как начальные точки заражения для этого последнего четвертого варианта. Один сайт, продвигающий программный генератор ключей, подмешивал пользователей, которые думали, что они загружают программный взлом, но на самом деле файл warez «содержал несколько файлов README и защищенный паролем архив, содержащий начальный дроппер для пакета вредоносных программ., 'setup_x86_x64_install.exe', - написал Proofpoint.

«Некоторые из аффилированных лиц, которые использовали [DanaBot], продолжили свои кампании, используя другое банковское вредоносное ПО (например, Ursnif и Zloader). Неясно, вызвало ли падение COVID-19, конкуренцию со стороны других банковских вредоносных программ, время на переработку или что-то еще, но похоже, что DanaBot вернулся и пытается восстановить свои позиции в мире угроз», - заключили исследователи». ***(Tom Spring. DanaBot Malware Roars Back into Relevancy // Threatpost (https://threatpost.com/danabot-malware-roars-back/163358/). 26.01.2021).***

***

«Вредоносная программа CursedGrabber проникла в репозиторий программного кода с открытым исходным кодом.

Три пакета вредоносного программного обеспечения были опубликованы в npm, репозитории кода, в котором разработчики JavaScript могут совместно использовать и повторно использовать блоки кода. Пакеты представляют угрозу цепочке поставок, поскольку они могут использоваться в качестве строительных блоков в различных веб-приложениях; По словам исследователей, любые приложения, поврежденные кодом, могут украсть токены и другую информацию у пользователей Discord.

Discord предназначен для создания сообществ в Интернете, называемых «серверами», либо в виде отдельных форумов, либо как часть другого веб-сайта. Пользователи общаются с помощью голосовых вызовов, видеозвонков, текстовых сообщений, мультимедиа и файлов. «Боты» Discord занимают центральное место в его функциях; это ИИ, которые могут быть запрограммированы для модерации дискуссионных форумов, приветствия и руководства новыми участниками, полицейских нарушителей правил и работы с сообществом. Они также используются для добавления на сервер функций, таких как музыка, игры, опросы, призы и многое другое.

Токены Discord используются внутри кода бота для отправки команд назад и вперед в Discord API, который, в свою очередь, контролирует действия бота. Если токен Discord украден, это позволит злоумышленнику взломать сервер.

Пакеты (с именами an0n-chat-lib, discord-fix и sonatype, все опубликованные scp173-deleted) были удалены, хотя неизвестно, сколько разработчиков

использовали их до того, как они были удалены. Sonatype сообщил Threatpost, что профиль пользователя был удален, а все пакеты были заменены заполнителями, чтобы злоумышленники не могли повторно обнаруживать вредоносное ПО под этими именами.

Хотя у «an0n-chat-lib» не было законного «двойного» пакета, два других использовали брэндджекинг и типосквоттинг, чтобы заставить разработчиков думать, что они легитимны.

Вредоносный компонент «discord-fix» называется аналогично легитимному «discord-XP», фреймворку XP для ботов Discord, и использует MongoDB. Пакет «sonatype» пока что основан на чистом брэндджекинге.

По словам исследователей Sonatype, есть также «явное свидетельство того, что в кампании вредоносного ПО использовался бот Discord для подсчета количества загрузок пакетов, чтобы сделать их более популярными для потенциальных пользователей».

По словам исследователей, авторы - те же операторы, что и вредоносная программа CursedGrabber Discord, и пакеты имеют общую ДНК с этой угрозой. «Вредоносная программа похожа, но с небольшими вариациями, чтобы попытаться избежать обнаружения», - сказал Threatpost в Sonatype.

Обнаруженное в ноябре вредоносное ПО CursedGrabber Discord нацелено на хосты Windows. Он содержит два файла .exe, которые вызываются и выполняются с помощью сценариев postinstall из файла манифеста package.json. Один из файлов .exe сканирует профили пользователей из нескольких веб-браузеров вместе с файлами Discord leveldb, крадет токены Discord, крадет информацию о кредитных картах и отправляет данные пользователя через веб-перехватчик злоумышленнику. Второй распаковывает дополнительный код с множеством возможностей, включая повышение привилегий, ведение кейлоггеров, создание снимков экрана, установку бэкдоров, доступ к веб-камерам и так далее.

В случае трех пакетов npm они «содержат варианты кода для кражи токенов Discord из вредоносного ПО Discord, которое Sonatype неоднократно обнаруживала», - сказал исследователь безопасности Sonatype Акс Шарма в пятничной публикации в блоге.

Вредоносное ПО с открытым исходным кодом, репозиторий

Загрузка вредоносных пакетов в репозитории кода становится все более распространенной тактикой, используемой операторами вредоносных программ. Например, в декабре RubyGems, репозиторий пакетов с открытым исходным кодом и менеджер для языка веб-программирования Ruby, был вынужден отключить два своих пакета программного обеспечения после того, как в них было обнаружено наличие вредоносного ПО.

Драгоценные камни содержали вредоносное ПО, которое постоянно запускалось на зараженных машинах Windows и заменяло любой адрес кошелька биткойнов или криптовалюты, который он нашел в буфере обмена пользователя, на злоумышленник. Итак, если пользователь поврежденного веб-приложения, созданного с использованием драгоценных камней, скопирует и вставит адрес кошелька получателя биткойнов где-нибудь в своей системе, адрес будет заменен на адрес злоумышленника.

«Мы неоднократно видели… вредоносные программы с открытым исходным кодом, поражающие GitHub, npm и RubyGems, злоумышленники могут использовать доверие в сообществе разработчиков ПО с открытым исходным кодом для доставки практически любых вредоносных программ, от сложных троянских программ- шпионов, таких как njRAT, до… CursedGrabber», - сказал Шарма Threatpost.

Последние результаты подтверждают, что атаки на цепочку поставок программного обеспечения будут становиться все более распространенными, и подчеркивают, насколько это важно для организаций, которые защищаются от таких атак и постоянно улучшают свои стратегии против них, согласно Sonatype». ***(Tara Seals. Discord-Stealing Malware Invades npm Packages // Threatpost (https://threatpost.com/discord-stealing-malware-npm-packages/163265/). 22.01.2021).***

***

«Компания Eset изучила банковский троян Vadokrist, который использует функционал бэкдора и распространяется через спам-сообщения, направленные преимущественно на финансовые учреждения Бразилии.

В отличие от большинства банковских троянов Vadokrist не собирает информацию о жертвах сразу после проникновения на их устройства. Однако в соответствии с исследованием Eset вредоносная программа имеет несколько функций схожих с ранее выявленным троянам Amavaldo, Casbaneiro, Grandoreiro и Mekotio.

Большинство латиноамериканских банковских троянов собирает информацию об устройстве жертвы во время первого запуска. Вредоносная программа Vadokrist получает имя пользователя только после начала атаки на определенное финансовое учреждение.

Несмотря на ограниченные возможности сбора информации, Vadokrist может управлять мышью, имитировать ввод с помощью клавиатуры, записывать нажатие клавиш, делать снимки экрана и перезагружать устройство. Также этот троян может блокировать доступ пользователей к банковским веб-сайтам посредством вмешательства в работу браузера, что позволяет злоумышленникам сохранить контроль над системой». ***(Банковский троян Vadokrist способен затаиться на компьютере жертвы // Компьютерное Обозрение(https://ko.com.ua/bankovskij_troyan_vadokrist_sposoben_zataitsya_na_kompyutere_zhertvy_136032). 22.01.2021).***

***

«В отчете, опубликованном на прошлой неделе фирмой Zscaler, она предупредила о новой угрозе для онлайновых Linux-серверов, которая является вариантом ботнета SystemdMiner, впервые обнаруженного в начале 2019 года.

Текущая версия была названа DreamBus, она отличается от SystemdMiner несколькими улучшениями. Ботнет нацелен на широкий круг приложений корпоративного уровня для машин Linux, в том числе на PostgreSQL, Redis, Hadoop YARN, Apache Spark, HashiCorp Consul, SaltStack и сервис SSH.

Некоторые из этих приложений взламываются методом грубой силы — перебором типичных администраторских логинов, другие — вредоносными командами, отправляемыми на открытые конечные точки API, или с помощью эксплойтов для более старых уязвимостей.

Таким образом DreamBus пытается закрепиться в Linux-сервере, чтобы позднее установить на нём приложение с открытым кодом, которое добывает криптовалюту Monero (XMR) для злоумышленников из этой преступной группы. Каждый из инфицированных серверов также используется как бот для запуска дальнейших атак на другие потенциальные жертвы.

По информации Zscaler, при создании DreamBus авторы приложили много усилий, чтобы всячески затруднить обнаружение ботнета. В частности, все системы, зараженные этим вредоносным ПО, обменивались данными с сервером управления и контроля (C&C) по новому протоколу DNS-over-HTTPS (DoH). Вредоносные программы, поддерживающие DoH, встречаются очень редко, так как они очень сложны в настройке…». ***(Ботнет DreamBus нацелен на корпоративные приложения на серверах Linux // Компьютерное Обозрение (https://ko.com.ua/botnet_dreambus_nacelen_na_korporativnye_prilozheniya_na_serverah_linux_136076). 26.01.2021).***

***

Програми-вимагачі

«Среди групп программ-вымогателей появляется новая тенденция, когда они уделяют первоочередное внимание краже данных с рабочих станций, используемых высшими руководителями и менеджерами, с целью получения «цельной» информации, которую они впоследствии могут использовать для давления и вымогательства у высшего руководства компании для утверждения крупных выплат выкупа.

ZDNet впервые узнал об этой новой тактике ранее на этой неделе во время телефонного разговора с компанией, которая заплатила многомиллионный выкуп банде вымогателей Clop.

Подобные звонки с другими жертвами Clop и интервью по электронной почте с компаниями, занимающимися кибербезопасностью, позже подтвердили, что это была не просто случайная случайность, а метод, который банда Clop отработала за последние несколько месяцев.

СДЕЛАТЬ ВЫМОГАТЕЛЬСТВО ЛИЧНЫМ

Этот метод является развитием того, что мы видели в последнее время у банд вымогателей.

За последние два года банды программ-вымогателей превратились из целевых групп в случайные атаки домашних потребителей в целенаправленные вторжения крупных корпораций.

Эти группы взламывают корпоративные сети, крадут важные файлы, которые могут попасть в их руки, шифруют файлы и затем оставляют записки о выкупе на разрушенных компьютерах.

В некоторых случаях записка о выкупе сообщает компаниям, что они должны заплатить выкуп, чтобы получить ключ дешифрования. В случае кражи данных некоторые записи о выкупе также информируют жертв о том, что, если они не уплатят выкуп, украденные данные будут опубликованы в Интернете на так называемых «сайтах утечки».

Группы программ-вымогателей надеются, что компании будут отчаянно пытаться избежать публикации в Интернете конфиденциальных данных или финансовых показателей, доступных для конкурентов, и будут с большей готовностью платить выкуп вместо восстановления из резервных копий.

В других случаях некоторые банды вымогателей заявляли компаниям, что публикация их данных также будет считаться утечкой данных, что во многих случаях также повлечет за собой штраф от властей, а также репутационный ущерб, чего компании также хотят избежать.

Однако банды программ-вымогателей не всегда могут получить доступ к конфиденциальным данным или конфиденциальной информации при всех осуществляемых ими вторжениях. Это снижает их способность вести переговоры и оказывать давление на жертв.

Вот почему во время недавних вторжений группа, которая часто использовала штамм вымогателя Clop, специально искала рабочие станции внутри взломанной компании, которые используются ее топ-менеджерами.

Группа просматривает файлы и электронные письма менеджера и извлекает данные, которые, по их мнению, могут быть полезны для угроз, смущения или давления на руководство компании - тех же людей, которые, скорее всего, будут отвечать за утверждение их требования выкупа через несколько дней.

«Это новый метод действий для злоумышленников, но я могу сказать, что не удивлен», - сказал ZDNet на этой неделе Стефан Тэнасе, эксперт по киберразведке из группы CSIS.

«Программы-вымогатели обычно используются в качестве «драгоценностей в короне» того бизнеса, на который они нацелены, - сказал Тэнасе. «Обычно это файловые серверы или базы данных, когда дело доходит до утечки данных с целью их утечки. Но для них имеет смысл пойти вслед за исполняемыми машинами, если это окажет наибольшее влияние».

CLOP УЖЕ ИСПОЛЬЗУЕТ ЭТУ ТАКТИКУ, REVIL ТОЖЕ, НО ВРЯД ЛИ

Бретт Кэллоу, аналитик угроз из компании Emsisoft, занимающейся кибербезопасностью, сказал ZDNet, что до сих пор они видели подобную тактику только в инцидентах, связанных с программой-вымогателем Clop.

«Этот стиль шантажа может быть modus operandi конкретного филиала [Clop], и этот филиал также может работать на другие группы [программ-вымогателей]», - сказал нам Кэллоу.

Аналитик Emsisoft охарактеризовал эту эволюцию тактики вымогательства как «совсем не удивительную» и «логическое и неизбежное развитие».

«За последние пару лет тактика, используемая группами программ-вымогателей, стала все более экстремальной, и теперь они используют все возможные методы давления на своих жертв», - сказал Кэллоу.

«Другие тактики включают запугивание и угрозы по телефону как руководителям, так и клиентам и деловым партнерам, рекламу в Facebook, работу с прессой и угрозы раскрыть «грязное белье» компаний».

Но из аналогичного интервью с Евгением Ерчовым, директором отдела реагирования на инциденты и информации о киберугрозах в Arete IR, выяснилось, что филиал REvil (Sodinokibi), занимающийся вымогательством как услуга, уже перенял эту технику от банды Clop (или это может быть тот же филиал Clop, о котором Келлоу упоминал выше).

«В частности, злоумышленник смог найти документы, относящиеся к текущим судебным разбирательствам и связанным с этим внутренним обсуждениям потерпевших», - сказал Эрчов ZDNet.

«Затем злоумышленник использовал эту информацию и напрямую связался с руководителями по электронной почте и пригрозил опубликовать данные о предполагаемом «неправомерном поведении руководства», - сказал Эрчов.

Аллан Лиска, старший архитектор безопасности в Recorded Future, сказал ZDNet, что они видели эту тактику только с атаками Clop, но они не исключают, что другие участники программ-вымогателей также применяют ее.

«Банды программ-вымогателей очень быстро осваивают новые методы, особенно те, которые повышают вероятность выплаты выкупа», - сказал Лиска.

"Это также имеет смысл в эволюции тактики вымогательства, поскольку банды вымогателей преследовали более крупные цели, им приходилось пробовать разные способы принудительного платежа.

«Утечка украденных данных - это то, о чем все знают, но были опробованы и другие методы, такие как REvil, пригрозивший электронным письмам с подробностями атаки на фондовые биржи», - сказал Лиска.

НЕ ВСЕГДА ПРАВДИВО

Однако Билл Сигел, генеральный директор и соучредитель фирмы по обеспечению безопасности Coveware, сказал, что во многих случаях данные, используемые в этих схемах вымогательства, нацеленных на руководство компании, не всегда правдивы или оправдывают ожидания.

«Они [группы программ-вымогателей] создают всевозможные угрозы относительно того, что они могут иметь, а что нет, - сказал Сигел ZDNet.

«Мы никогда не сталкивались со случаями, когда украденные данные действительно свидетельствовали бы о корпоративных или личных злоупотреблениях. По большей части, это просто тактика запугивания для увеличения вероятности оплаты», - сказал Сигел.

«Давайте помнить, что это преступные вымогатели. Они будут говорить или требовать всякие фантастические вещи, если это приносит им деньги» ***(Catalin Cimpanu. Some ransomware gangs are going after top execs to pressure companies into paying // ZDNet (https://www.zdnet.com/article/some-ransomware-gangs-are-going-after-top-execs-to-pressure-companies-into-paying/). 09.01.2021).***

***

«Федеральное бюро расследований США (ФБР) разослало компании частного сектора с предупреждением о том, что программа-вымогатель Egregor активно атакует и вымогает у компаний по всему миру.

ФБР сообщает в сообщении TLP: WHITE Private Industry Notification (PIN), опубликованном в среду, что Эгрегор утверждает, что уже нанес удар и скомпрометировал более 150 жертв с тех пор, как агентство впервые обнаружило эту вредоносную деятельность в сентябре 2020 года.

«Из-за большого количества участников, задействованных в развертывании Egregor, тактика, методы и процедуры (TTP), используемые при его развертывании, могут широко варьироваться, создавая серьезные проблемы для защиты и смягчения последствий», - заявляет служба разведки и безопасности США.

«Программа-вымогатель Egregor использует несколько механизмов для взлома бизнес-сетей, включая нацеливание на бизнес-сеть и личные учетные записи сотрудников, которые имеют общий доступ к бизнес-сетям или устройствам».

Фишинговые электронные письма с вредоносными вложениями и небезопасным протоколом удаленного рабочего стола (RDP) или виртуальными частными сетями являются одними из векторов атаки, используемых субъектами Egregor для получения доступа и горизонтального перемещения в сетях своих жертв.

Egregor использует Cobalt Strike, Qakbot / Qbot, Advanced IP Scanner и AdFind для повышения привилегий и бокового перемещения сети.

Аффилированные лица также используют 7zip и Rclone, иногда замаскированные под процесс Service Host Process (svchost), для кражи данных перед развертыванием полезных нагрузок вымогателей в сети жертв.

ФБР также опубликовало список рекомендуемых мер по смягчению последствий, которые должны помочь защитить от атак Эгрегора:

Резервное копирование критически важных данных в автономном режиме.

Убедитесь, что копии критически важных данных находятся в облаке, на внешнем жестком диске или устройстве хранения.

Защитите свои резервные копии и убедитесь, что данные недоступны для изменения или удаления из системы, в которой они хранятся.

Установите и регулярно обновляйте антивирусное или антивирусное программное обеспечение на всех хостах.

Используйте только безопасные сети и избегайте общедоступных сетей Wi-Fi.

Используйте двухфакторную аутентификацию и не нажимайте на незапрошенные вложения или ссылки в электронных письмах.

Приоритетное исправление общедоступных продуктов и приложений удаленного доступа, включая недавние уязвимости RDP (CVE-2020-0609, CVE-2020-0610, CVE-2020-16896, CVE-2019-1489, CVE-2019-1225, CVE-2019 -1224, CVE-2019-1108).

Просмотрите подозрительные файлы .bat и .dll, файлы с данными разведки (например, файлы .log) и инструменты для эксфильтрации.

Безопасно настройте RDP, ограничив доступ, используя многофакторную аутентификацию или надежные пароли.

Работа RaaS с бывшими филиалами Maze в качестве партнеров

Egregor - это программа-вымогатель как услуга, которая сотрудничает с аффилированными лицами, которые взламывают сети для развертывания полезных нагрузок вымогателей, распределяя доходы от выкупа с операторами Egregor с использованием разделения 70/30.

После проникновения в сети жертв они также крадут файлы перед шифрованием устройств и используют их в качестве рычага воздействия под угрозой публичной утечки украденных данных, если выкуп не будет уплачен.

Egregor начал работать после того, как Maze закрыл свою работу, и многие из филиалов Maze сразу же переключились на RaaS Egregor, как сообщили BleepingComputer злоумышленники.

С сентября аффилированные лица Egregor взламывают и шифруют системы нескольких известных организаций, включая, помимо прочего, Ubisoft, Kmart, Randstad, Barnes and Noble, Cencosud, Crytek и транспортное агентство Metro Vancouver TransLink.

Не платите выкуп, сообщайте об атаках программ-вымогателей

Жертвам также рекомендуется не платить выкуп, поскольку это не гарантирует успешного восстановления зашифрованных данных, а также финансирует их будущие операции и поощряет их продолжать свои атаки.

Агентство призывает жертв сообщать обо всех инцидентах с программами-вымогателями, в которых они участвуют, чтобы помочь следователям отследить стоящих за ними лиц, создающих угрозы, и предотвратить будущие атаки.

ФБР обратилось к компаниям и частным лицам, пострадавшим от программ-вымогателей, с просьбой в течение некоторого времени сообщать о любых заражениях, чтобы лучше понять угрозу и юридические причины для судебного преследования банд программ-вымогателей и их операторов.

OFAC (Управление по контролю за иностранными активами министерства финансов) заявило в прошлом году, что организации, помогающие жертвам программ-вымогателей выплачивать выкуп, также сталкиваются с рисками санкций, поскольку их действия могут нарушать правила OFAC.

Жертв убедили немедленно связаться с OFAC, если и когда они считают, что запрос на выплату вымогателя может включать в себя систему санкций, чтобы избежать потенциальных рисков санкций». ***(Sergiu Gatlan. FBI warns of Egregor ransomware extorting businesses worldwide // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fbi-warns-of-egregor-ransomware-extorting-businesses-worldwide/). 07.01.2021).***

***

«Исследователи безопасности, расследующие серию инцидентов с программами-вымогателями в нескольких компаниях, обнаружили вредоносное ПО, указывающее на то, что атаки могут быть результатом работы хакерской группы, которая, как считается, действует от имени Китая.

Хотя атакам не хватает изощренности, обычно присущей продвинутым злоумышленникам, есть веские доказательства их связи с APT27, группой, обычно участвующей в кампаниях кибершпионажа, также известной как TG-3390, Emissary Panda, BRONZE UNION, Iron Tiger и LuckyMouse.

Атаки произошли в 2020 году и были нацелены на как минимум пять компаний сектора онлайн-гемблинга, которые работают по всему миру и успешно зашифровали несколько основных серверов.

Хотя это были серьезные инциденты с вымогательством, злоумышленник использовал BitLocker, инструмент шифрования дисков в Windows, чтобы заблокировать серверы.

Исследователи из фирм по кибербезопасности Profero и Security Joes отреагировали на эти инциденты и обнаружили, что хакеры достигли своих целей через стороннего поставщика услуг, который был заражен через другого стороннего поставщика.

Анализ атак выявил образцы вредоносного ПО, связанные с DRBControl, кампанией, описанной ранее в этом году в отчете Trend Micro и приписываемой APT27 и Winnti, обе группы активны по крайней мере с 2010 года и связаны с китайскими хакерами. Если APT27 ориентирован на кибершпионаж, Winnti известен своей финансовой мотивацией.

В совместном отчете, опубликованном BleepingComputer, Profero и Security Joes делятся свидетельствами, указывающими на эти две группы, заявив, что они нашли образец бэкдора Clambling, аналогичный тому, который использовался в кампании DRBControl.

Они также обнаружили веб-оболочку ASPXSpy. Модифицированная версия этой вредоносной программы ранее была замечена в атаках, приписываемых APT27.

Другое вредоносное ПО, обнаруженное на зараженных компьютерах, включает троян удаленного доступа PlugX, который регулярно упоминается в отчетах о кибербезопасности о кампаниях, связанных с Китаем.

«Что касается того, кто стоит за этой конкретной цепочкой заражения, есть чрезвычайно сильные связи с APT27 / Emissary Panda с точки зрения сходства кода и TTP [тактики, техники и процедуры]», - говорится в отчете.

Хотя группа кибершпионажа, участвующая в финансово-мотивированной кампании, является необычной, эта атака будет не первым случаем, когда APT27 развертывает вымогательское ПО на системах-жертвах.

Исследователи из Positive Technologies приписали APT27 атаку программного обеспечения-вымогателя Polar с апреля 2020 года, основываясь на использовании вредоносного ПО, которое обычно используется этой группой.

Атаки против пяти компаний в секторе азартных игр не были особенно изощренными и основывались на известных методах уклонения от обнаружения и бокового действия.

В отчете Profero и Security Joes говорится, что злоумышленник развернул вредоносное ПО PlugX и Clambling в системной памяти, используя более старый исполняемый файл Google Updater, который был уязвим для боковой загрузки DLL.

Кроме того, злоумышленник воспользовался уязвимостью 2017 года (CVE-2017-0213) для повышения привилегий на машине. Код эксплойта для этой ошибки общедоступен.

Дэниел Банс, главный аналитик по безопасности в Security Joes, сказал BleepingComputer, что ключевой вывод из этих атак - участие группы кибершпионажа в финансовой кампании.

Омри Сегев Мойал, генеральный директор Profero, говорит, что дерзость такой злонамеренной группы является еще одним сигналом того, что правительства должны иметь единый подход в борьбе с этими угрозами.

Недавно другая группа хакеров, которая, как считается, работает на правительство, была связана с атаками программ-вымогателей. Согласно ClearSky, поддерживаемая Ираном хакерская группа Fox Kitten участвовала в операциях вымогателя Pay2Key против организаций в Израиле и Бразилии». ***(Ionut Ilascu. China's APT hackers move to ransomware attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/chinas-apt-hackers-move-to-ransomware-attacks/). 04.01.2021).***

***

«Согласно новому исследованию, почти половина всех утечек данных в больницах и в более широком секторе здравоохранения происходит в результате атак программ-вымогателей.

Вымогателей Банды все больше и больше добавляя дополнительный слой вымогательством к атакам не только путем шифрования сети и требуют сотни тысяч или даже миллионы долларов в Bitcoin, чтобы восстановить их, но и кражи конфиденциальной информации и угрожая опубликовать его, если выкуп не уплачивается.

Этот метод двойного вымогательства предназначен как дополнительный рычаг, чтобы заставить жертв атак программ-вымогателей уступить и заплатить выкуп, а не тратить время на восстановление сети самостоятельно. Для здравоохранения перспектива утечки данных в Интернете вызывает особую тревогу, поскольку она может включать конфиденциальные частные медицинские данные наряду с другими формами идентифицируемой личной информации пациентов.

Поэтому некоторые организации предпочтут заплатить выкуп, чтобы этого не произошло, в то время как другие не будут подчиняться требованиям вымогательства. В результате, согласно анализу исследователей кибербезопасности Tenable, теперь на долю программ-вымогателей приходится 46% утечек медицинских данных. Более 35% всех нарушений связаны с атаками программ-вымогателей, что зачастую приводит к огромным финансовым затратам.

Один из основных способов получения доступа к больничным сетям бандами программ-вымогателей - использование пары уязвимостей VPN, обнаруженных в контроллере Citrix ADC, влияющих на узлы шлюза (CVE-2019-19781) и Pulse Connect Secure (CVE-2019-11510).

Обе эти уязвимости получили исправления безопасности, чтобы к началу 2020 года хакеры не могли ими воспользоваться, но, несмотря на это, большое количество организаций еще не применили обновление.

Это позволило группам программ-вымогателей - и даже хакерским операциям, связанным с национальными государствами - использовать незащищенные уязвимости, чтобы закрепиться в сетях, и они будут продолжать делать это до тех пор, пока сети не получат необходимые исправления безопасности.

«По мере расширения поверхности атаки управление уязвимостями играет центральную роль в современных стратегиях кибербезопасности. Неисправленные уязвимости оставляют уязвимыми конфиденциальные данные и критически важные бизнес-системы и представляют прибыльные возможности для участников программ-вымогателей», - сказал Рено Дерасон, соучредитель и главный технолог Офицер Tenable.

Ключевым способом защиты сетей, ставших жертвами программ-вымогателей и других кибератак, является применение исправлений после их выпуска, особенно тех, которые предназначены для исправления критических уязвимостей. А если в вашей организации есть приложения, которые больше не получают обновлений безопасности, исследователи рекомендуют заменить это программное обеспечение альтернативным, которое все еще поддерживается.

«Если программные решения, используемые вашей организацией, больше не получают обновлений безопасности, обновление до одного с действующим контрактом на поддержку имеет жизненно важное значение», - говорится в отчете.

«Совершенно необходимо, чтобы организации выявляли активы в своей среде, которые уязвимы для недостатков, которым уже много месяцев или лет, и немедленно применяли соответствующие исправления», - говорится в заявлении». ***(Danny Palmer. Ransomware attacks now to blame for half of healthcare data breaches // ZDNet (https://www.zdnet.com/article/ransomware-attacks-now-to-blame-for-half-of-healthcare-data-breaches/). 15.01.2021).***

***

«Шотландское агентство по охране окружающей среды (SEPA) подтвердило в четверг, что некоторые из его контакт-центра, внутренние системы, процессы и внутренние коммуникации пострадали в результате атаки вымогателя, которая произошла в канун Рождества.

«SEPA подтверждает, что продолжающиеся атаки программ-вымогателей могут быть совершены серьезными и организованными киберпреступными международными группировками, намеревающимися нарушить работу государственных служб и вымогать государственные средства», - заявило агентство.

SEPA добавила, что после изоляции скомпрометированных систем восстановление, вероятно, займет «значительный период», и некоторые из зараженных систем SEPA необходимо будет заменить новыми.

Системы электронной почты также пострадали от атаки вымогателей в канун Рождества и все еще не работают, а некоторые внутренние системы и внешние информационные продукты будут отключены в краткосрочной перспективе.

«[Электронная] почта, расписания сотрудников, ряд специализированных инструментов для отчетности, системы и базы данных остаются недоступными, и существует вероятность того, что доступ к ряду систем и инструментов будет недоступен в течение длительного периода», - говорится в сообщении SEPA.

Однако агентство заверило общественность, что приоритетные услуги по регулированию, мониторингу, прогнозированию наводнений и предупреждению все еще работают, несмотря на последствия атаки.

Это расследование продолжается. Полиция Шотландии тесно сотрудничает с SEPA и нашими партнерами в правительстве Шотландии, а также с более широким сообществом правоохранительных органов Великобритании для расследования этого инцидента и оказания поддержки в ответ на него. Запросы остаются на ранней стадии и продолжают развиваться, включая использование специализированных ресурсов по киберпреступности для поддержки этого ответа. «В настоящее время было бы неуместно приводить более подробную информацию о расследованиях. - Детектив-инспектор Майкл МакКаллах из отдела расследований киберпреступлений полиции Шотландии.

Утечка украденных файлов программой-вымогателем Conti

Хотя SEPA не связывает атаку с какой-либо конкретной операцией вымогателя, банда вымогателей Conti заявляет об атаке и уже опубликовала 7% украденных данных на своем сайте утечки.

По данным SEPA, во время атаки было похищено около 1,2 ГБ данных, и есть свидетельства того, что по меньшей мере 4000 файлов были доступны и украдены.

«Хотя мы не знаем и, возможно, никогда не узнаем полной информации об украденных 1,2 ГБ информации, мы знаем, что первые признаки указывают на то, что кража информации связана с рядом сфер бизнеса», - сказал генеральный директор SEPA Терри А. - сказал Хирн.

«Часть украденной информации станет общедоступной, а часть - нет».

Информация, украденная операторами Conti во время атаки, включает:

Деловая информация: такая информация, как, но, возможно, не ограничиваясь, общедоступными регулируемыми разрешениями на сайты, разрешениями и уведомлениями о принудительном исполнении. Некоторая информация, относящаяся к корпоративным планам, приоритетам и программам изменений SEPA.

Информация о закупках: такая информация, как публично доступные награды за закупки, но не ограничивается ими.

Информация о проекте: Информация о нашей коммерческой работе с международными партнерами.

Информация о персонале: личная информация, относящаяся к персоналу SEPA.

SEPA в настоящее время работает со специалистами по кибербезопасности и экспертами из межведомственных партнеров, включая полицию Шотландии и

Национальный центр кибербезопасности, над задачами искоренения, устранения и восстановления.

«Быстро предприняв шаги по изоляции наших систем, специалисты по кибербезопасности, работающие с SEPA, правительством Шотландии, полицией Шотландии и Национальным центром кибербезопасности, теперь подтвердили значимость продолжающегося инцидента», - добавил А'Хирн.

«Партнеры подтвердили, что SEPA по-прежнему подвергается продолжающейся атаке программ-вымогателей, вероятно, со стороны международных серьезных и организованных киберпреступных групп, намеревающихся нарушить работу государственных служб и вымогать государственные средства». ***(Sergiu Gatlan. Scotland environmental regulator hit by 'ongoing' ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/scotland-environmental-regulator-hit-by-ongoing-ransomware-attack/). 14.01.2021).***

***

«Capcom выпустила новое обновление для расследования утечки данных и заявляет, что теперь до 390000 человек могут пострадать от ноябрьской атаки вымогателей.

2 ноября Capcom подверглась кибератаке со стороны программы-вымогателя Ragnar Locker, заявившей, что они украли у компании 1 ТБ данных. Операция вымогателя потребовала выкупа в размере 11 миллионов долларов в биткойнах, чтобы не раскрыть украденные файлы и не предоставить дешифратор.

Вскоре после утечки украденных данных Capcom компания Ragnar Locker сообщила, что они пострадали от утечки данных, в результате которой были раскрыты девять типов личной информации.

В опубликованном сегодня обновлении расследования Capcom заявляет, что они подтвердили 16 415 человек, чья личная информация была раскрыта, при возможном общем количестве пострадавших в 390 000 человек.

«В качестве дополнения к текущему расследованию компания подтвердила, что личная информация еще 16 406 человек была скомпрометирована, в результате чего общее число с момента начала этого расследования составляет 16 415 человек».

«Кроме того, компания также установила, что потенциальное максимальное количество клиентов, деловых партнеров, других внешних сторон и т. Д., Чья личная информация могла быть скомпрометирована в результате атаки, составляет около 390 000 человек», - говорится в последнем обновлении Capcom.

Capcom заявляет, что для подтвержденных 16 406 человек раскрытые данные могут представлять собой сочетание имен, адресов, номеров телефонов, информации НТ и адресов электронной почты…

Когда операции-вымогатели осуществляют свои атаки, они крадут почти все файлы и базы данных, которые могут попасть в их руки.

Банды вымогателей сообщили BleepingComputer, что они сохраняют более ценные данные для онлайн-аукционов или для использования в дальнейших атаках.

Это означает, что утечка данных может быть не всеми данными, которые они украли.

Следовательно, безопаснее предположить, что ваши данные были взломаны во время атаки, и внимательно следить за целевыми фишинговыми атаками. Хотя нет никаких указаний на то, что пароли были раскрыты, также рекомендуется изменить свой пароль Capcom, и, если он используется на других сайтах, также изменить их там». ***(Lawrence Abrams. Capcom: 390,000 people may be affected by ransomware data breach // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/capcom-390-000-people-may-be-affected-by-ransomware-data-breach/). 12.01.2021).***

***

«Ассоциация британских страховщиков (ABI) выступила за включение платежей от программ-вымогателей в полисы киберстрахования первой стороны.

В нем говорилось, что страхование не является «альтернативой» делать все возможное, чтобы сначала минимизировать риск.

Однако он добавил, что без прикрытия фирмы могут столкнуться с финансовым крахом.

Профессор Киаран Мартин, бывший глава Национального центра кибербезопасности, сказал, что Великобритании необходимо пересмотреть свою политику в отношении программ-вымогателей.

«Финансирование организованной преступности»

Программы-вымогатели - это разновидность вредоносного ПО, при котором зараженные компьютеры удаленно блокируются киберпреступниками, которые затем требуют выкуп, часто в виде биткойнов, чтобы разблокировать их и вернуть данные, которые они хранят.

Существует множество примеров компаний и государственных органов, которые решили платить, потому что у них нет резервных копий данных, или они не могут позволить - или не имеют времени - перестроить свои системы с нуля.

The Guardian сообщила, что профессор Мартин, который сейчас работает в Школе государственного управления им. Блаватника Оксфордского университета, сказал, что, по его мнению, страховщики «финансируют организованную преступность», принимая заявления о вымогательстве, но он сказал BBC, что проблема борьбы с программами-вымогателями намного шире, чем просто страхование сектор.

По его словам, хотя официальный совет заключается в том, чтобы не оплачивать спрос, это не является незаконным в Великобритании.

«Я немного симпатизирую страховщикам, потому что, пока это законно, есть стимулы платить».

Хотя требования выкупа могут быть высокими, альтернативные последствия также могут быть разрушительными.

Когда в 2019 году на глобального производителя алюминия Norsk Hydro было совершено нападение, это обошлось компании примерно в 45 миллионов фунтов стерлингов, а ее прибыль сразу после этого упала на 82%, сообщает Reuters.

Norsk Hydro отказалась оплачивать спрос, что, возможно, было бы дешевле, но у нее была страховка.

Представитель ABI сказал, что страховщики действительно требуют, чтобы были приняты «разумные меры предосторожности» для предотвращения успеха кибератак в первую очередь, точно так же, как автомобили и дома требуют принятия мер безопасности для сдерживания воров.

«Некоторые могут возразить, что любая страховка, покрывающая преступное деяние, может внушить страхователю ложное чувство безопасности», - сказал он.

Профессор Мартин сказал, что не думает, что запрет на страхование от программ-вымогателей обязательно решит проблему.

«Но это стоит серьезной консультации, потому что, если мы продолжим, как есть, все станет еще хуже», - сказал он». ***(Zoe Kleinman. Insurers defend covering ransomware payments // BBC (https://www.bbc.com/news/technology-55811165). 27.01.2021).***

***

«По словам лиц, ответственных за защиту организаций от взломов и кибератак, программы-вымогатели - самая большая проблема кибербезопасности, с которой сталкиваются предприятия.

Опрос руководителей информационной безопасности (CISO) и руководителей безопасности (CSO), проведенный фирмой Proofpoint, занимающейся кибербезопасностью, показал, что программы- вымогатели теперь рассматриваются как основная угроза кибербезопасности их организации в течение следующего года.

Почти половина - 46% - опрошенных ОГО и CISO заявили, что программы-вымогатели или другие формы вымогательства со стороны посторонних представляют самую большую угрозу кибербезопасности.

Программы-вымогатели продолжают оставаться одной из самых разрушительных и разрушительных кибератак, в то время как для киберпреступников шифрование сетей и требование биткойнов в обмен на ключ дешифрования - это самый простой способ быстро заработать большие деньги на взломанной сети.

Значительный процент организаций заплатит выкуп, который может составлять миллионы долларов, потому что они воспринимают это как самый быстрый способ восстановления сети и наименьшее количество дальнейших нарушений в бизнесе. И именно потому, что эти выкупы выплачиваются, программы-вымогатели остаются столь привлекательными и прибыльными для киберпреступников.

Некоторые из других кибератак, которые директора по информационной безопасности считают самой большой угрозой в этом году, включают взлом облачных учетных записей, внутренние угрозы, фишинг и атаки компрометации корпоративной электронной почты.

Хотя все эти киберугрозы не так заметны, как атаки программ-вымогателей, они также могут создавать проблемы для организаций, особенно если хакеры могут

комбинировать атаки, такие как фишинг, и компрометация учетных данных облачной учетной записи, чтобы получить дополнительный доступ к сетям.

Часто такие виды атак используются на ранних этапах попыток взлома сетей с помощью программ-вымогателей, поэтому защита сети от одной конкретной формы кибератаки может иметь большое значение для ее защиты и от других.

Помимо программ обучения и повышения осведомленности, организации могут помочь защитить себя от программ-вымогателей и других атак, применяя исправления безопасности по мере их выпуска, не позволяющие хакерам использовать известные уязвимости.

Использование дополнительной защиты, такой как двухфакторная аутентификация в организации, также может помочь предотвратить вредоносные атаки, поскольку хакерам будет намного сложнее перемещаться по сети, даже если у них есть правильные учетные данные». ***(Danny Palmer. Ransomware is now the biggest cybersecurity concern for CISOs // ZDNet (https://www.zdnet.com/article/ransomware-is-now-the-biggest-cybersecurity-concern-for-cisos/). 21.01.2021).***

***

«Агентство по кибербезопасности и безопасности инфраструктуры (CISA) объявило сегодня о кампании по снижению риска программ-вымогателей - целенаправленных, скоординированных и устойчивых усилиях, направленных на поощрение организаций государственного и частного секторов к внедрению передовых методов, инструментов и ресурсов, которые могут помочь им смягчить эту кибербезопасность. риск и угроза.

Программы-вымогатели все чаще угрожают как общедоступным, так и частным сетям, вызывая потерю данных, проблемы с конфиденциальностью и обходясь в миллиарды долларов в год. Эти инциденты могут серьезно повлиять на бизнес-процессы и оставить организации без данных, необходимых для работы и предоставления критически важных услуг. Со временем злоумышленники скорректировали свою тактику использования программ-вымогателей, включив в нее принуждение жертв к выплате путем угроз раскрыть украденные данные, если они откажутся платить, а также публичное наименование и опозорение жертв как вторичные формы вымогательства.

«CISA стремится работать с организациями на всех уровнях для защиты их сетей от угроз программ-вымогателей», - сказал Брэндон Уэльс, исполняющий обязанности директора CISA. «Это включает в себя совместную работу с нашими партнерами из государственного и частного секторов для понимания, разработки и своевременного обмена информацией о разнообразных и разрушительных угрозах программ-вымогателей. Любой человек может стать жертвой программы-вымогателя, поэтому каждый должен принять меры для защиты своих систем».

В рамках этой кампании, которая будет уделять особое внимание поддержке организаций, занимающихся реагированием на COVID-19, и учебных заведений K-12, CISA работает над повышением осведомленности о важности борьбы с программами-вымогателями как части передовых методов организации в области кибербезопасности и защиты данных. В течение следующих нескольких месяцев

CISA будет использовать свои платформы социальных сетей для повторения ключевых моделей поведения или действий со ссылками на ресурсы, которые могут помочь техническим и нетехническим партнерам бороться с атаками программ-вымогателей.

CISA создала новый универсальный ресурс cisa.gov/ransomware. На этой странице заинтересованные партнеры найдут четыре категории ресурсов вымогателей:

Оповещения и заявления: официальные обновления CISA, чтобы помочь заинтересованным сторонам защититься от постоянно меняющейся среды угроз вымогателей. Эти предупреждения предназначены для системных администраторов и другого технического персонала, чтобы повысить уровень безопасности их организации.

Руководства и услуги: советы и передовые методы для домашних пользователей, организаций и технического персонала по защите от растущей угрозы программ-вымогателей.

Информационные бюллетени и инфографика: простая в использовании и понятная информация, помогающая организациям и частным лицам лучше понять угрозы и последствия атаки программ-вымогателей.

Тренинги и вебинары: эта информация предоставляет техническую и нетехническую аудиторию, включая менеджеров, руководителей предприятий и технических специалистов, с организационной точки зрения и стратегическим обзором.

Многие ресурсы на этой веб-странице были разработаны в сотрудничестве с отраслевыми и межведомственными партнерами, например:

Совместное руководство по программам -вымогателям CISA и Межгосударственного центра обмена и анализа информации (MS-ISAC) ;

Совместные рекомендации CISA, Федерального бюро расследований (ФБР) и Министерства здравоохранения и социальных служб (HHS) по кибербезопасности в отношении деятельности программ-вымогателей, нацеленных на сектор здравоохранения и общественного здравоохранения;

CISA, ФБР, Отдел расследований внутренней безопасности DHS и Секретная служба США записали видео-обсуждение тенденций и прогнозов в отношении программ-вымогателей с Национального саммита по кибербезопасности CISA 2020.

Информационный бюллетень CISA о киберугрозах для дистанционного обучения школьников до 12 лет для нетехнических специалистов в области образования при участии ФБР». ***(CISA LAUNCHES CAMPAIGN TO REDUCE THE RISK OF RANSOMWARE // Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/news/2021/01/21/cisa-launches-campaign-reduce-risk-ransomware). 21.01.2021).***

***

«…лондонское рекламное агентство, среди клиентов которого Atlantic Records, Suzuki и Penguin Random House, было сброшено в Интернет бандой вымогателей.

The7stars, базирующаяся в лондонском Вест-Энде, подала [PDF] выручку в размере 379,36 млн фунтов стерлингов по сравнению с 326 млн фунтов стерлингов, брутто-счета в размере 426 млн фунтов стерлингов и чистую прибыль в размере 2,1 млн фунтов стерлингов за год, закончившийся 31 марта 2020 года.

В тех же отчетах, поданных в Регистрационную палату Великобритании, он хвастался своей позицией как «крупнейшее независимое медиа-агентство в Великобритании, имеющее существенное значение», что делает его привлекательной мишенью для вымогателей-вымогателей Clop.

Атака, похоже, произошла после 15 декабря, когда годовая отчетность The7stars была подготовлена для подачи в Регистрационную палату. Хотя в документе подробно говорится о его хороших финансовых показателях, в нем ничего не говорится о киберрисках или атаках.

На скриншотах, опубликованных на сайте Tor банды Clop, показаны сканы паспортов, счетов-фактур, что-то вроде фотографии с вечеринки сотрудников и, по иронии судьбы, «соглашение о защите данных».

Публикация украденных файлов на веб-сайте группы вымогателей обычно является индикатором того, что требование выкупа было отклонено, хотя более агрессивная тактика, применявшаяся в прошлом году, включает упреждающую утечку украденных данных в качестве очевидного стимула для быстрой выплаты марками.

В список клиентов агентства входят бывший лейбл Led Zeppelin Atlantic Records, японский производитель мотоциклов Suzuki и британские железнодорожные операторы, в том числе Great Western Railway. Маловероятно, что эти компании будут напрямую затронуты, хотя похоже, что Clop хочет создать впечатление, что он украл коммерчески конфиденциальные документы, касающиеся клиентов The7stars.

Представитель ICO направил нам заявление: «Мы получили отчет от the7stars об атаке программы-вымогателя, и мы делаем запросы, чтобы оценить предоставленную информацию».

Мы попросили комментарий у The7stars.

Как мы сообщали в прошлом году, когда та же банда вымогателей напала на немецкую компанию Software AG, преступники Clop были заметно настойчивее, чем другие, использующие то же мошенничество с кражей и вымогательством.

Бретт Кэллоу, аналитик угроз в компании Emsisoft, сказал нам в то время: «Clop - это вариант CryptoMix и может использоваться группой, стоящей за банковским трояном Dridex. Подобно REvil и NetWalker, он в основном используется для нацеливания на корпоративные сети, с известными жертвами в прошлом, включая Prominent и ExecuPharm». Он добавил, что требования Клопа могут исчисляться миллионами.

По сути, борьба с программами-вымогателями сводится к тому, чтобы сделать бизнес-модель неэкономичной. С этой целью отказ от подкупа мошенников (и обеспечение того, чтобы ваша страховая компания не платила от вашего имени) - это первый шаг, который нужно сделать, и примеру Шотландского агентства по охране окружающей среды следует следовать примеру отрасли. ®

Обновлено для добавления

«Мы можем подтвердить, что недавно мы столкнулись с ИТ-инцидентом в форме изощренной атаки с использованием программ-вымогателей», - сказал The Register представитель the7star.

«Мы смогли восстановить наши системы из резервных копий и продолжаем расследование в качестве абсолютного приоритета. Впоследствии лица, ответственные за эту преступную деятельность, опубликовали информацию, извлеченную из наших систем, в Интернете. Мы поддерживаем тесные связи с нашими клиентами, чтобы предложить нашу постоянную поддержку и сообщили в полицию». ***(Gareth Corfield. Clop ransomware gang clips sensitive files from Atlantic Records' London ad agency The7stars, dumps them online // The Register (https://www.theregister.com/2021/01/22/the7stars_ransomware_attack_clop/). 22.01.2021).***

***

«Банда программ-вымогателей продолжает насмехаться над IObit, разработчиком программного обеспечения для Windows, взламывая свои форумы, чтобы показать требование выкупа.

16 января форумы IObit были взломаны в рамках атаки по распространению вымогателя DeroHE. Во время этой атаки злоумышленники разослали по электронной почте всем пользователям форума IObit рекламную акцию по бесплатному программному обеспечению со ссылкой на установщик вымогателей, размещенный на форумах IObit.

Когда получатели загружали поддельный установщик программного обеспечения IObit, они были заражены вымогателем DeroHE. Чтобы получить доступ к дешифратору, злоумышленники требуют 100 долларов в криптовалюте DERO, или IObit может заплатить им 100000 долларов в DERO для расшифровки всех жертв.

DeroHE - первая программа-вымогатель, требующая оплаты в DERO, что, вероятно, будет способствовать продвижению криптовалюты и увеличению ее стоимости.

DERO описывает себя как монету конфиденциальности, которая обеспечивает безопасные и анонимные транзакции и выполнение смарт-контрактов.

«Dero - это первый криптопроект, сочетающий блокчейн Proof of Work со структурой блока DAG и полностью анонимными транзакциями», - говорится на сайте DERO.

Банда вымогателей насмехается над IObit в продолжении хакеров на форуме

Во время нашего первоначального отчета DeroHE форум все еще был взломан с помощью скриптов рекламного ПО, которые перенаправляли пользователей на сайты для взрослых при нажатии на ссылки.

На выходных злоумышленники снова взломали форумы IObit, чтобы отобразить сообщение с требованием, чтобы IObit заплатил им 100 000 долларов в DERO, иначе атаки будут продолжены.

«Здравствуйте, ваш IObit был взломан! Прошла неделя, а ваша «антивирусная» компания все еще ничего не делает для защиты своего сервера!

IObit прислал нам 100000 DERO или больше хаков и утечек», - читали на форуме IObit в выходные.

Сегодня IObit, похоже, закрыл свои форумы, вероятно, пытаясь очистить его от любых веб-оболочек и исправить уязвимости. Время ожидания попыток подключения к форуму…». ***(Lawrence Abrams. Ransomware gang taunts IObit with repeated forum hacks // Bleeping Computer (https://www.bleepingcomputer.com/news/security/ransomware-gang-taunts-iobit-with-repeated-forum-hacks/). 25.01.2021).***

***

«Крупный паназиатский оператор розничной сети Dairy Farm Group в этом месяце подвергся атаке вымогателя REvil. Злоумышленники утверждают, что потребовали выкуп в размере 30 миллионов долларов.

Группа компаний Dairy Farm Group управляет более чем 10 000 торговых точек и насчитывает 230 000 сотрудников по всей Азии. В 2019 году общий годовой объем продаж Dairy Farm Group превысил 27 миллиардов долларов.

Группа управляет многочисленными продуктовыми брендами, магазинами товаров повседневного спроса, товаров для здоровья, товаров для дома и ресторанами на азиатских рынках, включая Wellcome, Giant, Cold Storage, Hero, 7-Eleven, Rose Pharmacy, GNC, Mannings, Ikea, Maxims и др.

Атака программ-вымогателей REvil на молочную ферму

На этой неделе с BleepingComputer связался злоумышленник, который заявил, что группа вымогателей REvil взломала сеть и зашифрованные устройства Dairy Farm Group примерно 14 января 2021 года.

BleepingComputer сообщили, что сумма выкупа составляет 30 миллионов долларов, но не подтвердила эту сумму независимо.

Чтобы доказать, что у них есть доступ к сети Dairy Farm, злоумышленник поделился снимком экрана консоли Active Directory Users and Computers MMC.

Злоумышленники утверждают, что через семь дней после атаки все еще имеют доступ к сети, в том числе полный контроль над корпоративной электронной почтой Dairy Farm, которая, по их утверждениям, будет использоваться для фишинговых атак.

«Они не могут закрыть свою сеть, потому что их бизнес остановится. Есть группа партнеров Revil, которые все еще атакуют эту компанию, там более 30 тысяч хостов», - сказал злоумышленник BleepingComputer.

Dairy Farm подтвердила BleepingComputer, что в этом месяце они подверглись кибератаке, но сообщила, что пострадали менее 2 процентов всех устройств компании.

«В Dairy Farm защита наших систем является главным приоритетом. В четверг мы выявили инцидент, затронувший менее 2 процентов наших бизнес-серверов. Они были отключены и изолированы. В качестве дополнительной меры предосторожности мы инициировали полную и тщательное расследование при поддержке внешнего специалиста по безопасности, введены дополнительные меры безопасности и дополнительно укреплены наши системы мониторинга».

«Все наши магазины открыты, торгуют и обслуживают наших клиентов на всех рынках, и закрываются только там, где есть ограничения COVID-19, введенные национальными или местными правительствами», - сообщили BleepingComputer в Dairy Farm по электронной почте.

В более позднем телефонном разговоре с Dairy Farm BleepingComputer сообщил компании, что злоумышленники утверждают, что все еще имеют доступ, и якобы все еще загружают данные из сети.

Компания заявила, что ей не было известно о краже каких-либо данных во время атаки, хотя скриншоты, которые видел BleepingComputer, показывают, что злоумышленники продолжали иметь доступ к электронной почте и компьютерам после атаки.

Например, ниже приведено внутреннее электронное письмо от Dairy Farm о кибератаке, допущенной злоумышленниками.

Поскольку REvil известен тем, что крадет данные во время атаки, а затем угрожает выпустить их, если выкуп не будет заплачен, неудивительно, что утечка украденных данных произошла позднее.

После рождественских праздников банды вымогателей, похоже, отдыхали от крупномасштабных атак. К сожалению, этот перерыв закончился, и количество атак на крупные предприятия снова увеличивается, как это было видно из атаки на молочную ферму и продолжающейся глобальной кибератаки на производителя кранов Palfinger». ***(Lawrence Abrams. Pan-Asian retail giant Dairy Farm suffers REvil ransomware attack // Bleeping Computer (https://www.bleepingcomputer.com/news/security/pan-asian-retail-giant-dairy-farm-suffers-revil-ransomware-attack/). 26.01.2021).***

***

«Другая банда вымогателей теперь использует DDoS-атаки, чтобы заставить жертву связаться с ними и договориться о выкупе.

В октябре 2020 года мы сообщили, что банды вымогателей начали использовать DDoS-атаки против сети или веб-сайта жертв в качестве дополнительного инструмента, чтобы заставить их платить выкуп. В то время двумя операциями, использующими эту новую тактику, были SunCrypt и RagnarLocker.

Распределенная атака типа «отказ в обслуживании» (DDoS) - это когда злоумышленник наводняет веб-сайт или сетевое соединение большим количеством запросов, чем он может обработать, что делает службу недоступной.

Когда компания подвергается атаке программы-вымогателя, многие жертвы восстанавливаются из резервных копий и не связываются с злоумышленниками.

Банда программ-вымогателей Avaddon теперь использует DDoS-атаки, чтобы уничтожить сайт или сеть жертвы, пока жертва не свяжется с ними и не начнет переговоры.

«Кроме того, их сайт в настоящее время подвергается DDoS-атаке, мы будем атаковать его, пока они не свяжутся с нами», - заявил Аваддон на своем сайте утечки данных программ-вымогателей.

Для одной из жертв, которую Avaddon в настоящее время выполняет DDoS-атаку, вы можете видеть, что веб-сайт больше не доступен.

Аналитик угроз Emsisoft Бретт Кэллоу, который поделился этой разработкой с BleepingComputer,

«Нет ничего удивительного в том, что злоумышленники сочетают в себе программы-вымогатели и DDoS-атаки: DDoS-атаки дешевы, просты и в некоторых случаях могут помочь убедить некоторые компании в том, что скорейшие платежи - наименее болезненный вариант. Чем больше давления преступники могут оказать на компании, тем увеличивают их шансы на получение оплаты», - сказал Келлоу BleepingComputer по электронной почте.

Когда Maze представил стратегию двойного вымогательства, другие банды вымогателей быстро переняли этот метод. Еще слишком рано говорить, будут ли злоумышленники применять DDoS-атаки аналогичным образом». ***(Lawrence Abrams. Another ransomware now uses DDoS attacks to force victims to pay // Bleeping Computer (https://www.bleepingcomputer.com/news/security/another-ransomware-now-uses-ddos-attacks-to-force-victims-to-pay/). 24.01.2021).***

***

«Больница CHwapi в Бельгии страдает от кибератаки, в ходе которой злоумышленники утверждают, что зашифровали 40 серверов и 100 ТБ данных с помощью Windows Bitlocker.

В воскресенье на Чвапи произошло нападение, в результате которого больница перенаправила пациентов в другие больницы и отложила хирургические процедуры.

В то время как услуги больницы медленно восстанавливаются и хирургические операции возобновляются, CHwapi продолжает отменять некоторые услуги и перенаправлять неотложные случаи в другие больницы.

Согласно бельгийскому СМИ L'Avenir, CHwapi подвергся атаке в воскресенье в 20:46, когда злоумышленники зашифровали 80 из 300 серверов, но больница не получила требования о выкупе.

Злоумышленники утверждают, что используют Windows BitLocker

Во вторник с BleepingComputer связались злоумышленники, заявившие, что они несут ответственность за атаку на CHwapi.

По словам злоумышленников, они использовали Windows BitLocker для шифрования 40 серверов и 100 ТБ данных. После шифрования устройств злоумышленники заявляют, что оставили записки с требованием выкупа под названием ransom.txt на контроллерах домена и серверах резервного копирования.

«Мы напали на больницу Чвапи в Бельгии 2 дня назад и установили на серверах записку о выкупе. Но ИТ-менеджеры не передали эту информацию руководству больницы. Руководство больницы выпустило пресс-релиз и сообщило, что записки о выкупе нет, но это ложь. что-то происходит", - написали злоуышленники BleepingComputer по электронной почте.

Вместо традиционных программ-вымогателей эта группа использует стандартное программное обеспечение, такое как Windows BitLocker и DiskCryptor,

для шифрования файлов и блокировки доступа к разделам диска с помощью пароля.

Злоумышленники сообщили BleepingComputer, что они не шифруют все устройства в сети, а только целевые серверы, содержащие большие объемы файлов, такие как файловые серверы и серверы резервного копирования.

Чтобы общаться с жертвами, эта группа хакеров создает записки о выкупе, содержащие идентификатор Bitmessage, который можно использовать для переговоров о выкупе…

Эта группа заявляет, что они не являются частью программы-вымогателя как услуги (RaaS) и не крадут и не утекают данные.

Некоторые банды вымогателей заявили, что они будут избегать шифрования больниц и предоставят бесплатный дешифратор, если они будут зашифрованы.

Когда мы спросили злоумышленников, будут ли они следовать аналогичной политике и предоставить больнице CHwapi бесплатный расшифровщик, мы не получили четкого ответа…». ***(Lawrence Abrams. CHwapi hospital hit by Windows BitLocker encryption cyberattack // Bleeping Computer (https://www.bleepingcomputer.com/news/security/chwapi-hospital-hit-by-windows-bitlocker-encryption-cyberattack/). 21.01.2021).***

***

«В 2020 году операторы вымогательского ПО прибегли к стратегии двойного вымогательства, в рамках которой злоумышленники крадут незашифрованные файлы жертв, а затем угрожают опубликовать их, если не будет уплачен выкуп. Используя данные, собранные с помощью автоматических каналов, специалисты компании Digital Shadows зафиксировали 550 сообщений о двойном вымогательстве на сайтах утечек данных, поддерживаемых более чем десятком вымогательских группировок.

По словам специалистов, программы-вымогатели теперь являются стандартным подходом для монетизации скомпрометированных компаний. Как обнаружили эксперты из CrowdStrike, более половины всех действий ее клиентов были направлены на устранение последствий атак программ-вымогателей. Количество компаний, ежегодно подвергающихся атакам вымогательского ПО, остается стабильным — 51% предприятий признали факт атаки вымогателей за последний год. Три четверти подобных атак успешно шифруют некоторые данные жертв.

Эксперты также отметили, что 66% от всех уведомлений о программах-вымогателях поступали от организаций и компаний в Северной Америке.

Согласно отчету Digital Shadows о киберугрозах за третий квартал 2020 года, на долю операторов Maze приходилась треть всех зафиксированных атак с использованием программ-вымогателей. В октябре прошлого года группировка прекратила свою преступную деятельность, и партнеры Maze перешли на использование вымогательского ПО под названием Egregor. Предположительно, Egregor представляет собой то же программное обеспечение, что и Maze и Sekhmet, поскольку они используют одинаковые записки с требованиями о выкупе, одинаковые названия сайтов платежей и имеют большую часть одного и того же

кода. В последнем квартале 2020 года на долю Egregor приходилась треть атак с использованием вымогателей, включая атаки на Barnes & Noble, производителя игр Ubisoft и Epicor Software.

Digital Shadows отслеживает сайты утечек данных, которые вымогательские группировки используют для публикации украденной информации. По данным компании, на сайты шести Maze, Egregor, Conti, Sodinokibi, DoppelPaymer и Netwalker пришлось 84% взломов в 2020 году». ***(Стратегия двойного вымогательства набирает популярность у киберпреступников // SecurityLab.ru (https://www.securitylab.ru/news/515993.php). 27.01.2021).***

***

Програми-трояни

«Группа хакеров из Северной Кореи использует троян RokRat в новой волне кампаний против правительства Южной Кореи.

Троян удаленного доступа (RAT) был связан с атаками, основанными на эксплойте текстового процессора на корейском языке, обычно используемого в Южной Корее в течение нескольких лет; в частности, компрометация документов Hangul Office (.HWP).

В прошлом вредоносное ПО использовалось в фишинговых кампаниях, которые привлекали жертв с помощью электронных писем, содержащих вложения на политическую тему, например, объединение Кореи и права человека Северной Кореи.

Считается, что RokRat - дело рук APT37, также известного как ScarCruft, Reaper и Group123. Активная, по крайней мере, с 2012 года расширенная постоянная группа угроз (APT), вероятно, спонсируется государством и, возможно, ей поручено нацеливаться на объекты, представляющие ценность для правящей партии Северной Кореи.

По словам исследователя безопасности Malwarebytes Хосейна Джази, в то время как предыдущие кампании были сосредоточены на использовании файлов .HWP, новый образец фишингового документа, относящийся к APT37, показывает поворот в тактике группы.

В сообщении в блоге на этой неделе компания, занимающаяся кибербезопасностью, описала обнаружение нового вредоносного документа, загруженного в Virus Total 7 декабря. В образце файла утверждается, что это запрос на встречу, датированный началом 2020 года, из чего следует, что атаки произошли в прошлом году.

Malwarebytes сообщает, что содержимое файла также указывает на то, что он «использовался для нацеливания на правительство Южной Кореи».

Документ не следует традиционному пути .HWP APT37; вместо этого встроенный макрос использует метод самодекодирования VBA для декодирования себя в память Microsoft Office. Это означает, что вредоносному ПО не нужно записывать себя на диск, возможно, чтобы избежать обнаружения.

После взлома Microsoft Office заглушка распаковщика встраивает вариант RokRat в программное обеспечение Notepad. Согласно Malwarebytes, этот метод позволяет без особых усилий обойти «несколько механизмов безопасности».

«Насколько нам известно, это впервые для этой APT-группы», - говорит Джази.

Чтобы обойти систему безопасности Microsoft, которая предотвращает динамическое выполнение макроса, злоумышленникам сначала необходимо обойти объектную модель VB (VBOM), изменив значения реестра.

Вредоносный макрос проверит, можно ли получить доступ к VBOM, и попытается установить ключ реестра VBOM в единицу, если его нужно обойти. В зависимости от результатов проверки, например, если настройка VBOM уже была пропущена, содержимое макроса также может быть запутано, деобфусцировано и затем выполнено в памяти.

Основная функция полезной нагрузки - создать модуль, использующий шелл-код для взлома Блокнота перед вызовом зашифрованного файла, размещенного на Google Диске, который содержит RokRat.

После развертывания на уязвимой машине RokRat сосредоточится на сборе данных из системы перед их отправкой в контролируемые злоумышленником учетные записи с облачными сервисами, включая Pcloud, Dropbox, Box и Яндекс. Вредоносная программа способна красть файлы, делать снимки экрана, захватывать учетные данные и вмешиваться в файловые каталоги.

RokRat - это вариант вредоносного ПО, которое также будет пытаться поддерживать скрытность, проверяя песочницы и наличие VMWare, сканируя отладочное программное обеспечение и анализируя библиотеки DLL, связанные с Microsoft и iDefense.

В новостях на этой неделе исследователи Trustwave недавно обнаружили новую фишинговую кампанию, которая развертывает QRat на машинах Windows. Этот троянец, впервые обнаруженный в 2015 году, обладает широкими возможностями обфускации и удаленного доступа». ***(Charlie Osborne. North Korean hackers launch RokRat Trojan in campaigns against the South // ZDNet (https://www.zdnet.com/article/north-korean-hackers-launch-rokrat-trojan-in-campaigns-against-the-south/). 07.01.2021).***

***

«Волна атак на компании в Колумбии использует троянов удаленного доступа (RAT) для кражи конфиденциальных данных.

Кампания, получившая название Operation Spalax, была раскрыта исследователями ESET во вторник.

В своем сообщении в блоге компания по кибербезопасности сообщила, что государственные и частные организации в Колумбии являются мишенью исключительно для злоумышленников, которые, похоже, проявляют особый интерес к энергетической и металлургической отраслям.

ESET начала отслеживать кампанию, которая продолжается, во второй половине 2020 года, когда по крайней мере 24 IP-адреса - вероятно,

скомпрометированные устройства, выступающие в качестве прокси-серверов для командных серверов (C2) злоумышленников - были связаны с потоком атак.

Чтобы начать цепочку заражения против целевой сущности, злоумышленники используют традиционный метод: фишинговые электронные письма. Темы этих мошеннических сообщений варьируются от требований присутствовать на судебных слушаниях до предупреждений о замораживании банковских счетов и уведомлений о прохождении обязательного теста на COVID-19.

В некоторых выборках выдавались агентства, в том числе Генеральная прокуратура (Fiscalia General de la Nacion) и Национальное налоговое и таможенное управление (DIAN).

К каждому электронному письму прикреплен файл .PDF, связанный с архивом .RAR. Если жертва загружает пакет, расположенный на OneDrive, MediaFire и других службах хостинга, исполняемый файл внутри запускает вредоносное ПО.

Злоумышленники используют набор дропперов и упаковщиков для развертывания полезных нагрузок троянца, цель которых - выполнить RAT, внедрив его в законный процесс.

Все три полезные нагрузки доступны на коммерческой основе и не были разработаны кибератаками собственными силами.

Первый - это Remcos, вредоносное ПО, доступное на подпольных форумах всего за 58 долларов. Второй RAT - это njRAT, троянец, последний раз замеченный в кампаниях, использующих Pastebin в качестве альтернативы структурам C2, а третий - AsyncRAT, инструмент удаленного администрирования с открытым исходным кодом.

«Между дропперами и полезными нагрузками нет однозначной связи, поскольку мы видели разные типы дропперов, выполняющих одну и ту же полезную нагрузку, а также один тип дропперов, подключенных к разным полезным нагрузкам», - отмечает ESET. «Однако мы можем утверждать, что дропперы NSIS в основном отбрасывают Remcos, а упаковщики Agent Tesla и AutoIt обычно сбрасывают njRAT».

RAT могут обеспечивать удаленный контроль доступа к злоумышленникам, а также содержать модули для кейлоггеров, захвата экрана, сбора содержимого буфера обмена, эксфильтрации данных, а также загрузки и выполнения дополнительных вредоносных программ, среди других функций.

По данным ESET, нет никаких конкретных указаний на атрибуцию, однако есть некоторые совпадения с APTC36, также известным как Blind Eagle. Этот APT был связан с атаками в 2019 году на колумбийские организации с целью кражи конфиденциальной информации.

Использование злоумышленником динамических DNS-сервисов означает, что инфраструктура кампании также постоянно меняется: новые доменные имена регистрируются для использования против колумбийских компаний на регулярной основе.

ESET также отметила ссылки на исследования, проведенные Trend Micro в 2019 году. Фишинговая тактика аналогична, но в то время как отчет Trend Micro

касается шпионажа и, возможно, целевого использования финансовых счетов, ESET не обнаружила какого-либо использования полезных данных, кроме кибершпионажа. Однако компания признает, что некоторые из целей текущей кампании, в том числе лотерейное агентство, не имеют логического смысла только для шпионской деятельности.

Фирма, занимающаяся кибербезопасностью, добавила, что из-за большой и быстро меняющейся инфраструктуры этой кампании мы должны ожидать, что в обозримом будущем эти атаки будут продолжаться в регионе». ***(Charlie Osborne. Colombian energy, metal firms under fire in new Trojan attack wave // ZDNet (https://www.zdnet.com/article/colombian-energy-metal-firms-under-fire-from-new-trojan-attack-wave/). 12.01.2021).***

***

Операції правоохоронних органів та судові справи проти кіберзлочинців

«Тюрина признали виновным по нескольким пунктам обвинения. В конечном счёте судья Лаура Суэйн, занимавшаяся разбирательством этого дела, поддержала об винение и вынесла приговор, в соответствие с которым Тюрину придётся провести в американской тюрьме 144 месяца. Как она полагает, Тюрин был вовлечен в "масштабную преступную деятельность финансового характера". Он якобы причастен к кибератакам на крупные американские компании с целью получения "данных клиентов".

Кроме того, россиянин должен выплатить США $19 214 956, именно такую прибыль по мнению суда он сумел извлечь за время своей криминальной деятельности. Отдельное слушание на тему возмещения ущерба назначено на 6 апреля 2021 года.

"Условия содержания россиянина под стражей были тяжелыми в контексте пандемии COVID-19, которым А. Тюрин заразился в американской тюрьме. Генконсульство России в Нью-Йорке держит на контроле дело Тюрина и находится в контакте с правоохранительными органами США", - отметили в консульстве.

Россиянина экстрадировали в США из Грузии в сентябре 2018 года. Ему инкриминируются взломы компьютерных систем, в том числе финансовых структур, брокерских контор и СМИ, публикующих финансовую информацию. Отмечалось, что за эти преступления он мог получить до 92 лет тюрьмы.

Изначально россиянин заявлял о своей невиновности в киберпреступлениях в сентябре 2018 года. Спустя год он пошел на сделку с прокуратурой, признав вину по нескольким пунктам обвинения. Секретная служба США утверждала, что он с сообщниками «присвоили сотни миллионов долларов». ***(Суд в США приговорил россиянина Андрея Тюрина к 12 годам тюрьмы за хакерство и сетевое мошенничество // SecurityLab.ru (https://www.securitylab.ru/news/515321.php). 08.01.2021).***

***

«Международная правоохранительная операция привела к закрытию того, что Европол называет крупнейшим в мире нелегальным рынком в даркнете.

DarkMarket, который насчитывал почти 500000 пользователей, был отключен после совместных усилий властей Германии, Австралии, Дании, Молдовы, Украины, Великобритании через Национальное агентство по борьбе с преступностью и США, включая ФБР. Европол заявил, что поддерживает Германию в координации трансграничных совместных усилий с участием международных партнеров.

В заявлении Европола говорится, что более 2400 продавцов на рынке в основном торгуют наркотиками и продают поддельные деньги, украденные или поддельные данные кредитных карт, анонимные SIM-карты и вредоносное ПО.

В нем говорится, что DarkMarket обработал более 320000 транзакций, из которых более 4650 биткойнов и 12800 монеро были переведены на подпольную торговую площадку на общую сумму примерно 140 миллионов евро - немногим более 170 миллионов долларов.

Гражданин Австралии был арестован в немецком городе Ольденбурге Центральным следственным управлением на выходных. Утверждается, что 34-летний австралиец является оператором DarkMarket.

По словам Европола, расследование, которое возглавило подразделение по борьбе с киберпреступностью при прокуратуре Кобленца, позволило офицерам определить местонахождение и закрыть рынок, выключить серверы и захватить криминальную инфраструктуру. Изъятая криминальная инфраструктура включала более 20 серверов в Молдове и Украине.

По словам Европола, проверка серверов, вероятно, приведет к дальнейшим расследованиям в отношении модераторов, продавцов и покупателей…» ***(Asha Barbaschow. Australian man arrested for alleged operation of now-shuttered DarkMarket // ZDNet (https://www.zdnet.com/article/australian-man-arrested-for-alleged-operation-of-now-shuttered-darkmarket/). 12.01.2021).***

***

«Русского хакера, замешанного в одной из крупнейших краж пользовательских данных из одного финансового института в истории США, заключили под стражу.

Житель Москвы Андрей Тиурин участвовал в международной хакерской кампании, целью которой были компьютерные системы крупнейших финансовых организаций, брокерские фирмы и новостные агентства с умыслом кражи данных.

Исходя из данных следствия, 37-летний москвич взламывал системы организаций между 2012 и серединой 2015 года и украл персональные данные более 100 миллионов клиентов компаний.

Среди жертв были E*Trade, Scottrade, the Wall Street Journal и JPMorgan Chase and Co., у которых хакер украл данные более 80 миллионов клиентов банка.

В США Тиурина экстрадировали в 2018 году из Грузии, 7 января его приговорили к 144 месяцам тюрьмы, а также выплате дополнительных $19 млн».

(Хакера, взломавшего JPMorgan Chase, осудили на 12 лет // SecureNews (https://securenews.ru/jpmorgan-chase-hacker-jailed-for-12-years/). 11.01.2021).

***

«Самый распространенный и опасный ботнет вредоносного ПО в мире был отключен после глобальной операции правоохранительных органов, планирование которой длилось два года.

Европол, ФБР, Национальное агентство по борьбе с преступностью Великобритании и другие скоординировали действия, в результате которых следователи взяли под свой контроль инфраструктуру, контролирующую Emotet, что стало одним из самых значительных нарушений киберпреступных операций за последние годы.

Emotet впервые появился в качестве банковского трояна в 2014 году, но превратился в одну из самых мощных форм вредоносного ПО, используемого киберпреступниками.

Emotet устанавливает бэкдор в компьютерные системы Windows с помощью автоматических фишинговых писем, которые распространяют документы Word, скомпрометированные с помощью вредоносного ПО. Темы электронных писем и документов в кампаниях Emotet регулярно меняются, чтобы обеспечить максимальную вероятность соблазнения жертв открывать электронные письма и устанавливать вредоносные программы - обычные темы включают счета, уведомления о доставке и информацию о COVID-19.

Те, кто стоит за Emotet, сдают в аренду свою армию зараженных машин другим киберпреступникам в качестве шлюза для дополнительных атак вредоносного ПО, включая инструменты удаленного доступа (RAT) и программы-вымогатели.

Это привело к Emotet становится то, что Европол описывает как «наиболее опасными вредоносное ПО в мире» и «один из самых значительных ботнетов за последнее десятилетие», операции, как Ryuk вымогателей и TrickBot банковского трояна нанимая доступ к машинам скомпрометирована Emotet для того, чтобы установить собственное вредоносное ПО.

Таким образом, уничтожение Emotet представляет собой одно из самых значительных действий против вредоносных программ и киберпреступников за последние годы.

«Это, вероятно, одна из самых значительных операций с точки зрения воздействия, которое мы оказали за последнее время, и мы ожидаем, что это окажет серьезное влияние», - сказал ZDNet Фернандо Руис, руководитель операций Европейского центра киберпреступности Европола (EC3). «Мы очень довольны».

За неделю действий правоохранительных органов по всему миру удалось получить контроль над инфраструктурой Emotet, состоящей из сотен серверов по всему миру, и нарушить ее изнутри.

Машины, зараженные Emotet, теперь направляются в инфраструктуру, контролируемую правоохранительными органами, а это означает, что киберпреступники больше не могут использовать взломанные машины, и

вредоносное ПО больше не может распространяться на новые цели, что приведет к значительному нарушению киберпреступных операций.

«Emotet был нашей угрозой номер один в течение долгого времени, и устранение этого будет иметь важное значение. Emotet участвует в 30% атак вредоносного ПО; успешное устранение будет иметь важное влияние на криминальную среду», - сказал Руис.

«Мы ожидаем, что это окажет влияние, потому что мы удаляем одну из основных дропперов на рынке - наверняка будет пробел, который другие преступники попытаются заполнить, но на некоторое время это окажет положительное влияние на кибербезопасность», - добавил он.

Расследование Emotet также обнаружило базу данных украденных адресов электронной почты, имен пользователей и паролей. Люди могут проверить, не был ли взломан Emotet их адрес электронной почты, посетив веб-сайт Национальной полиции Нидерландов.

Европол также работает с группами реагирования на компьютерные чрезвычайные ситуации (CERT) по всему миру, чтобы помочь тем, кто, как известно, заражен Emotet.

Чтобы защитить себя от вредоносных программ, таких как Emotet, Европол рекомендует использовать антивирусные инструменты вместе с полностью обновленными операционными системами и программным обеспечением, чтобы киберпреступники не могли использовать известные уязвимости для доставки вредоносного ПО. Также рекомендуется, чтобы пользователи прошли обучение по вопросам кибербезопасности, чтобы помочь идентифицировать фишинговые электронные письма.

Удаление Emotet является результатом более чем двухлетней скоординированной работы правоохранительных органов по всему миру, включая Национальную полицию Нидерландов, Федеральную полицию по борьбе с преступностью Германии, Национальную полицию Франции, Бюро криминальной полиции Литвы, Королевскую канадскую конную полицию, США. Федеральное бюро расследований, Национальное агентство по борьбе с преступностью Великобритании и Национальная полиция Украины.

Расследование Emotet и выявление киберпреступников, ответственных за его запуск, все еще продолжается». ***(Danny Palmer. Emotet: The world's most dangerous malware botnet was just disrupted by a major police operation // ZDNet (https://www.zdnet.com/article/emotet-worlds-most-dangerous-malware-botnet-disrupted-by-international-police-operation/). 27.01.2021).***

***

«Кирилл Викторович Фирсов, гражданин России, сегодня признал себя виновным в федеральном суде в киберпреступности, признав, что он был администратором веб-сайта, который обслуживал киберпреступников, виртуально продавая такие предметы, как украденные данные кредитной карты, другая личная информация и услуги, которые будут использоваться для преступной деятельности.

Согласно соглашению о признании вины, Фирсов получал хорошую оплату как администратор DEER.IO, онлайн-платформы, обслуживающей киберпреступников. DEER.IO была российской платформой, которая позволяла преступникам создавать интернет-магазины и продавать незаконные товары или услуги. DEER.IO начал свою деятельность как минимум в октябре 2013 года, и по состоянию на март 2020 года у него было около 3000 магазинов с продажами, превышающими 17 миллионов долларов.

DEER.IO предложила под ключ дизайн витрины и хостинговую платформу, с помощью которой киберпреступники могли рекламировать и продавать свои продукты, такие как собранные учетные данные, взломанные серверы и услуги, такие как помощь в выполнении целого ряда кибер-хакерских действий. Как подробно описано выше, преступник может просто «зарегистрироваться» «настроить кошельки для получения средств», «загрузить продукты» и «получить деньги».

После того, как преступник заплатил за открытие своего магазина на платформе DEER.IO, сайт затем направил новоиспеченного владельца магазина через автоматическую настройку, чтобы загрузить продукты и услуги, предлагаемые через магазин, и настроить кошельки с криптовалютой для собирать платежи за приобретенные товары и / или услуги. Киберпреступник, который хотел продавать контрабанду или предлагать криминальные услуги через DEER.IO, мог приобрести витрину прямо на сайте DEER.IO за 800 рублей (примерно 12,50 долларов США) в месяц. Ежемесячная плата оплачивалась биткойнами или различными российскими онлайн-способами оплаты, такими как WebMoney, российская система денежных переводов, аналогичная PayPal.

Владелец магазина имел возможность приобрести название витрины, связанное с DEER.IO или одним из его субдоменов, например DEER.ST, DEER.IS или DEER.EE (например, https: // [SHOP NAME] .deer.io, например как ONLYFB.DEER.IO, SHIKISHOP.DEER.IO и SELLACCSS.DEER.IS) или произвольное имя (например, https: // [НАЗВАНИЕ МАГАЗИНА], такое как SQLBAZAR.SHOP и ISIS.RENTS.HOUSE), которые направил потенциального покупателя к инфраструктуре витрины, размещенной на DEER.IO.

Киберпреступник, который хотел совершить покупку в витринах на веб-сайте DEER.IO, мог использовать веб-браузер для перехода к домену DEER.IO, который содержал функцию поиска, которая позволяла людям искать в каталоге определенные товары или просматривать популярные витрины, содержащие товары для покупка. Любые покупки производились с использованием криптовалюты, такой как биткойн, или через российские системы денежных переводов. Например, как указано выше, киберпреступник может приобрести украденные учетные записи Uber со связанной информацией о кредитной карте у SHIKISHOP.DEER.IO. Чтобы совершить эти покупки, потенциальному покупателю просто нужно было щелкнуть корзину в правой части экрана.

Первоначальное сканирование витрин DEER.IO выявило тысячи скомпрометированных учетных записей, выставленных на продажу, в том числе файлы с персональной информацией (PII), содержащие полные номера социального

страхования США, даты рождения и адреса жертв. Многие из этих жертв находились в Европе и Соединенных Штатах, в том числе жертвы в Сан-Диего.

Судья Синтия Башант должна вынести приговор Фирсову 12 апреля 2021 года.

«Это был универсальный магазин для преступников, - сказал прокурор США Роберт Брюэр. «Киберпреступность - одна из самых распространенных угроз, с которыми сталкивается наша страна. Данные украдены и продаются в Dark Web каждый день, и мы выделяем значительные ресурсы на борьбу с этой серьезной проблемой». Брюэр высоко оценил отличную работу помощника прокурора США Александры Ф. Фостер и агентов ФБР по этому делу.

«Интернет позволяет киберпреступникам и нашим противникам атаковать американцев новыми и неожиданными способами. Поэтому ФБР постоянно старается опережать меняющийся характер киберугроз», - сказала Сюзанна Тернер, специальный агент, отвечающий за полевой офис ФБР в Сан-Диего. «Захват веб-сайта DEER.IO и осуждение Фирсова являются примером исследовательского мастерства и юрисдикционной способности киберпрограммы ФБР для выявления, обнаружения и привлечения к ответственности любого, кто пытается извлечь выгоду из ущерба, нанесенного гражданам, предприятиям и инфраструктуре США.» ***(Russian Hacker Pleads Guilty to Administering a Website that Catered to Criminals // Department of Justice (https://www.justice.gov/usao-sdca/pr/russian-hacker-pleads-guilty-administering-website-catered-criminals). 21.01.2021).***

***

«Темные веб-сайты, связанные с операцией вымогателя Netwalker, были захвачены правоохранительными органами США и Болгарии.

Netwalker - это программа-вымогатель как услуга (RaaS), которая начала свою работу в конце 2019 года, и ее аффилированные лица привлекаются для распространения программ-вымогателей и заражения жертв в обмен на 60-75% долю выкупа.

Эта операция с программным вымогателем оказалась очень прибыльной для злоумышленников: согласно августовскому отчету, они заработали 25 миллионов долларов всего за пять месяцев.

Сегодня сайты платежей и утечки данных программы-вымогателя Netwalker были захвачены правоохранительными органами и теперь отображают уведомление об аресте от ФБР и болгарских правоохранительных органов.

В уведомлении об изъятии говорится, что задержание было проведено Министерством юстиции США, ФБР, Болгарской национальной следственной службой и Генеральным управлением Болгарии по борьбе с организованной преступностью.

«Этот скрытый сайт был захвачен Федеральным бюро расследований в рамках скоординированных действий правоохранительных органов, направленных против программы-вымогателя NetWalker».

"Это действие было предпринято в координации с прокуратурой Соединенных Штатов по центральному округу Флориды и отделом компьютерных преступлений и интеллектуальной собственности Министерства юстиции при

существенной поддержке со стороны Болгарской национальной следственной службы и Главного управления по борьбе с организованной преступностью, "говорится в уведомлении об изъятии веб-сайта.

На данный момент ФБР не опубликовало никакой информации о взломе, поэтому неясно, смогли ли правоохранительные органы получить ключи дешифрования в рамках этой операции или были ли произведены аресты.

Поскольку Netwalker является одним из наиболее активных семейств программ-вымогателей, доступ к ключам дешифрования может позволить многим жертвам бесплатно восстановить свои файлы.

Восстановление ключей дешифрования также стало бы огромной победой для правоохранительных органов, поскольку операции с программами-вымогателями были чрезвычайно устойчивы к нарушениям.

Некоторые из громких жертв, на которые нацелена Netwalker, включают Equinix, Enel Group, иммиграционное агентство Аргентины, Калифорнийский университет в Сан-Франциско (UCSF) и K-Electric.». ***(Lawrence Abrams. Netwalker ransomware dark web sites seized by law enforcement // Bleeping Computer (https://www.bleepingcomputer.com/news/security/netwalker-ransomware-dark-web-sites-seized-by-law-enforcement/). 27.01.2021).***

***

Технічні аспекти кібербезпеки

«Более 80 процентов из 650 специалистов по кибербезопасности и ИТ, опрошенных Check Point Software Technologies в июле, заявили, что их традиционные решения безопасности либо вообще не работают, либо предоставляют только ограниченные функции в облаке.

По словам Т. Дж. Гонена, главы линейки облачных продуктов компании, это указывает на то, что миграция и развертывание облачных технологий в организациях опережают возможности их групп безопасности по защите от атак и взломов.

«Их существующие решения безопасности обеспечивают лишь ограниченную защиту от облачных угроз, и командам часто не хватает опыта, необходимого для улучшения процессов безопасности и соответствия требованиям», - сказал Гонен.

Отставание в безопасности и эффективности

Однако проблема не в недостатке инструментов. Gartner прогнозирует, что глобальные расходы на инструменты облачной безопасности в 2020 году составят 585 миллионов долларов, что на 33 процента больше, чем в 2019 году.

«Мы участвуем в гонке кибервооружений, которая спровоцировала гонку инструментов безопасности с развивающимися атаками злоумышленников, вынуждающими нас тратить больше, чтобы попытаться защитить себя», - сказал Джим Ривис, соучредитель и генеральный директор Cloud Security Alliance (CSA). который способствует использованию лучших практик кибербезопасности в облачных вычислениях.

«Наш ответ по умолчанию - использовать новые инструменты, чтобы не отставать, но мы проигрываем эту гонку, поскольку противники продолжают опережать защитников», - заявил Ривис. «Мы увеличиваем операционные расходы и расходы на персонал, но каким-то образом снижаем безопасность и эффективность. Наши сложные и дорогостоящие операции на самом деле увеличивают вероятность успеха злоумышленников».

CSA определила то, что, по его мнению, является критическим пробелом, - это отсутствие возможности легко использовать и объединять выходные данные инструментов безопасности с развернутой аналитикой угроз.

Пять проблем мешают развитию этой способности:

Быстрые темпы изменений как в технологиях безопасности, так и в противниках;

Поставщики сосредотачиваются на «единой стеклянной панели» или информационной панели, которая визуально представляет данные о событиях. Проблема здесь в том, что обилие и разнообразие данных о событиях и темпах вредоносной активности нелегко представить на одной информационной панели. Таким образом, покупатели не хотят использовать одну панель, потому что они потратили средства на обучение различным продуктам безопасности, которые они используют.

Нет легко реализуемого протокола обмена и онтологии маркировки данных.

Интеграция и обработка разрозненных наборов данных из разных инструментов безопасности и источников информации затруднена из-за разных форматов и протоколов, управления дубликатами и исправлениями, а также важности понимания контекста; и

Переход от использования программного обеспечения и продуктов к защищенным системам к сосредоточению внимания на данных, генерируемых системами данных.

Комментарии CSA «действительны в целом, но не должны восприниматься как общее заявление», - сказал TechNewsWorld Сару Найяр, генеральный директор компании Gurucul, занимающейся глобальной безопасностью и анализом мошенничества.

«Концептуально, одна стеклянная панель может напрямую отображать всю важную информацию», - утверждает она. «Это позволяет аналитикам сосредоточиться на том, что является наиболее важным для их работы. Правильно настроенная единая панель представляет соответствующую информацию в одном месте в зависимости от роли каждого пользователя и позволяет пользователю детализировать конкретные события, риски, угрозы и т. Д., по мере необходимости - без потери контекста и необходимости менять инструменты».

Новый подход к облачной безопасности

ИТ-отделам необходимо «разорвать цикл, установленный двадцать лет назад, и заложить новый краеугольный камень киберзащиты: облачную защиту, ориентированную на данные», - заявило в прошлом месяце CSA.

Использование ориентированной на данные защиты, интеграции и автоматизации инструментов и общей архитектуры требует пересмотра того, что означает интеллект в контексте кибербезопасности, создания киберпамяти и

создания и поддержания безопасных интеллектуальных экосистем, говорится в документе.

Разведка «должна быть определена как способность организации нормализовать, преобразовывать и автоматически извлекать полезные сведения и контекст из инструментов внутренней безопасности и внешних источников, чтобы сократить среднее время на обнаружение и реагирование».

Создание киберпамяти включает в себя вызов данных о событиях, собранных как из внутренних средств безопасности, так и из внешних угроз, вместо того, чтобы обрабатывать каждое событие отдельно. Машинное обучение следует использовать для выявления закономерностей для более эффективного и действенного противодействия вредоносной активности.

Безопасные интеллектуальные экосистемы - это облачные банки памяти, которые непрерывно объединяют и обогащают данные из внутренних инструментов безопасности и внешних источников. Эти расширенные данные могут автоматически обновлять инструменты киберзащиты или проводить сортировку для дальнейших действий аналитиков. Данные из отдельной экосистемы могут быть переданы другим компаниям или организациям для формирования совместной оборонной экосистемы.

«Это не призыв к единственному продукту, а новый образ мышления для использования «интеллекта» для интеграции и автоматизации рабочих процессов с данными из инструментов и источников безопасности, используемых внутри и между предприятиями для создания интеллектуальных экосистем», - говорится в документе.

По словам Гонена из Check Point, предприятиям «необходимо получить целостную видимость во всех своих общедоступных облачных средах и развернуть унифицированные автоматизированные средства защиты, обеспечивающие соответствие нормативным требованиям и анализ событий». «Таким образом, они могут идти в ногу с потребностями бизнеса, обеспечивая при этом постоянную безопасность и соответствие требованиям». ***(Richard Adhikari. Cloud Security Practices Playing Into Hands of Attackers // ECT News Network, Inc. (https://www.technewsworld.com/story/86964.html). 07.01.2021).***

***

«Агентство национальной безопасности США опубликовало сегодня руководство по преимуществам и рискам зашифрованных протоколов DNS, таких как DNS-over-HTTPS (DoH), которые стали широко использоваться за последние два года.

Агентство по кибербезопасности США предупреждает, что, хотя такие технологии, как DoH, могут шифровать и скрывать запросы DNS пользователей от сетевых наблюдателей, они также имеют недостатки при использовании в корпоративных сетях.

«DoH не является панацеей», - говорится в сообщении АНБ по безопасности [PDF], опубликованном сегодня, утверждая, что использование протокола дает компаниям ложное ощущение безопасности, повторяя многие аргументы, представленные в статье ZDNet на DoH в октябре. 2019.

Агентство национальной безопасности заявило, что DoH не полностью предотвращает возможность злоумышленникам видеть трафик пользователя и что при развертывании внутри сетей его можно использовать для обхода многих инструментов безопасности, которые для обнаружения угроз используют анализ классического (открытого текста) трафика DNS.

Кроме того, АНБ утверждает, что многие из сегодняшних серверов DNS-преобразователей с поддержкой DoH также размещаются на внешних серверах, вне контроля компании и ее возможностей для аудита.

АНБ: ИСПОЛЬЗУЙТЕ СОБСТВЕННЫЕ ПРЕОБРАЗОВАТЕЛИ DOH, А НЕ СТОРОННИЕ

АНБ призывает компании избегать использования зашифрованных технологий DNS в своих собственных сетях или, по крайней мере, использовать сервер распознавания DNS с поддержкой DoH, который размещен внутри компании и находится под их контролем.

Более того, АНБ утверждает, что этот же совет следует применять и к классическим DNS-серверам, а не только к зашифрованным / DoH-серверам.

«АНБ рекомендует, чтобы трафик DNS корпоративной сети, зашифрованный или нет, отправлялся только назначенному преобразователю DNS», - говорится в сообщении агентства.

«Это обеспечивает правильное использование основных средств управления безопасностью предприятия, облегчает доступ к локальным сетевым ресурсам и защищает внутреннюю сетевую информацию.

«Все другие преобразователи DNS должны быть отключены и заблокированы», - заявило агентство безопасности.

CISA ВЫПУСТИЛА АНАЛОГИЧНОЕ ПРЕДУПРЕЖДЕНИЕ В ПРОШЛОМ ГОДУ.

Но не только АНБ требует осторожности в отношении зашифрованного DNS, такого как DoH, но и его аналога, DoT (DNS-over-TLS).

В апреле прошлого года Агентство по кибербезопасности и безопасности инфраструктуры также выпустило директиву, в которой всем федеральным агентствам США предлагается отключать DoH и DoT внутри своих сетей из-за угроз безопасности.

CISA посоветовал агентствам подождать, пока его инженеры не смогут предоставить официальный правительственный преобразователь DoH / DoT, который снизит любые угрозы отправки правительственного трафика DoH / DoT сторонним поставщикам DNS.

Сообщение АНБ также появилось после того, как иранские кибершпионы были замечены, используя DoH для эксфильтрации данных из взломанных сетей, не будучи обнаруженными.

Кроме того, бесплатные инструменты, выпущенные на GitHub, также сделали тривиальным перехват зашифрованных соединений DoH для сокрытия украденных данных и обхода классического защитного программного обеспечения на основе DNS». ***(Catalin Cimpanu. NSA warns against using DoH inside enterprise networks // ZDNet (https://www.zdnet.com/article/nsa-warns-against-using-doh-inside-enterprise-networks/). 14.01.2021).***

***

«Квантовые компьютеры гораздо мощнее привычных нам устройств и способны показывать высокие результаты в различных областях жизни. Вместе с тем их взлом может моментально обрушить цифровые системы в критически важных инфраструктурах.

СТО научно-производственной компании QRate и директор центра компетенций НТИ «Квантовые коммуникации» в МИСиС Юрий Курочкин рассказывает, как крупный бизнес и государственные структуры готовятся к атакам с применением квантового компьютера и что для этого необходимо.

Гости из будущего

Квантовые технологии (квантовый компьютер, квантовые коммуникации и квантовые сенсоры) постепенно выходят из лабораторий в реальный мир. Новые научные открытия помогают в продвижении и коммерциализации технологии. В начале этого года MIT включил квантовый интернет в топ-10 прорывных технологий 2020 года. Уже сегодня любой желающий может получить облачный доступ к квантовому компьютеру IBM. Его разработчики считают, что так можно найти множество разных сценариев применения новой технологии и ускорить ее развитие. Предполагается, что квантовые компьютеры превзойдут классические по многим параметрам. Они принесут невероятные результаты в медицине, промышленности и других отраслях.

Вместе с этим такие мощности откроют дорогу для беспрецедентных киберпреступлений. Дело в том, что для защиты данных во многих сферах чаще всего используют асимметричную криптографию, неустойчивую к атакам с участием квантового компьютера. Квантовый взлом обрушит все привычные цифровые системы в телекоме, IT, банковском секторе, медицине и других критически важных инфраструктурах.

Возможно, вмешательство в цифровые операции с использованием квантовых компьютеров кажется эпизодом из будущего. Однако злоумышленники могут украсть данные уже сейчас, а расшифровать их позже, когда инновационная вычислительная техника выйдет из лабораторий в частное пользование.

Сегодня разные отрасли осознают эту опасность и заранее готовят защиту, не дожидаясь появления универсального квантового компьютера, достаточно мощного как для решения полезных задач, так и взлома криптографии.

Вокруг новых способов передачи данных, способных выдержать квантовые атаки, формируется реальный рынок. В первую очередь это квантовые коммуникации, а именно — квантовое распределение криптографических ключей (Quantum key distribution или QKD).

Эта технология использует квантовые свойства элементарных частиц — фотонов — для того, чтобы защитить передачу информации на уровне фундаментальных законов физики.

Сегодня мировой объем рынка QKD оценивается в $ 3 млрд. А к 2030 году может вырасти до $ 17, 3 млрд.

Квантовые коммуникации (QC) — это направление, в рамках которого разрабатываются технологии или методы передачи информации, закодированной в

квантовые состояния. Одним из направлений квантовых коммуникаций является квантовое распределение ключей, которое обеспечивает гарантированную на уровне законов физики защиту передаваемой информации.

Поэтому многие государственные структуры и крупный бизнес действуют на опережение: исследуют угрозы, внедряют квантово-безопасные криптографические решения и планируют заработать на этом. Например, Toshiba анонсировала партнерство с телекоммуникационными компаниями Verizon Communication Inc в США и BT Group в Великобритании. Корпорация планирует выручить на решениях для защиты от квантовых угроз $3 млрд к 2030 году.

Интерес к квантовым коммуникациям на разных уровнях подчеркивают громкие пилотные проекты в телекоммуникационной и банковской отраслях. Параллельно идет процесс стандартизации технологии в рамках NIST (Национальный институт стандартов и технологий США).

Защита для мобильного интернета

Пользователи могут даже не замечать, сколько транзакций в день они совершают. Электронные платежи, входы в личные кабинеты, регистрации в социальных сетях, общение в мессенджерах: в момент передачи персональные данные крайне уязвимы. Поэтому важным для этого года стал кейс телекоммуникационного гиганта SK Telecom, который анонсировал чипсет с квантовым генератором случайных чисел (QRNG) от производителя ID Quantique. Технология встроена в смартфон Samsung Galaxy A Quantum 5G. Таким образом производители предполагают повысить безопасность персональных данных пользователей в интернете будущего. Например, обезопасить вход в учетные записи, операции с электронным кошельком, проведение мобильных платежей. Амбициозный пилот заявлен как первый опыт коммерциализации квантовых технологий для мобильных телефонов.

Устройством уже заинтересовался корейский банк DGB Daegu. Транзакции, которые клиенты проводят через банковское приложение на смартфоне Samsung Galaxy A Quantum 5G, будут защищены при помощи шифрования на основе истинно непредсказуемых случайных чисел.

Эта реакция закономерна. McAfee и CSIS подсчитали, что в 2020 году хакерские атаки нанесли мировой экономике ущерб больше чем в $1 трлн.

Квантовая защита для волоконно-оптических линий связи

Другим вектором атак могут стать магистральные линии связи. Поскольку по ним передаются стратегически важные данные. Копирование и взлом этих данных может привести к убыткам в миллиарды рублей. Перед IT службами стоит сложная и важная задача — интегрировать в высоконагруженные каналы криптографические решения, устойчивые к перспективным атакам, в том числе квантового компьютера.

Эти решения требуют:

интеграции высокоскоростных аппаратных шифраторов на симметричных ключах;

квантового распределения ключей, которое обеспечивает эти шифраторы секретными ключами.

Для передачи одиночных фотонов необходима выделенная жила оптоволокна. Так как часто сети перегружены, ученые работают над тем, чтобы квантовый и классический сигналы могли сосуществовать в одном оптоволокне на разных длинах волн.

Одним из самых громких проектов в России стал пилот волоконно-оптической линии связи с применением технологии квантового распределения ключей шифрования (QKD), которая соединила два офиса госкорпорации «Росатом» в Москве. Пилотный проект был проведен при поддержке ПАО «Ростелеком» на оборудовании научно-производственной компании QRate. В момент тестирования ученые имитировали разрыв квантового канала, при котором отработал буфер хранения секретных ключей. Успешное тестирование подтвердило требуемый уровень надежности для внедрения действующего решения в сетевую инфраструктуру.

Квантовую сеть длинной в 800 км планирует создать компания ОАО «РЖД», которая отвечает за реализацию дорожной карты развития высокотехнологичной области «Квантовые коммуникации» в России. Представители компании говорят о планах развития рынка и новых видов бизнеса на основе квантовых коммуникаций.

Тренд квантовой защиты в телекоммуникациях поддерживают корпорации-гиганты в отрасли связи по всему миру. Свои мощности для изучения ограничений технологии квантового распределения ключей предоставила немецкая телекоммуникационная компания Deutsche Telekom (DT). Испытательный стенд будет включать 100-километровую волоконно-оптическую сеть DT. Берлинский пилот станет частью большого проекта консорциума OPENQKD, который параллельно реализуется в нескольких европейских странах. Основная цель проекта — подготовиться к появлению квантовых вычислителей, способных взломать криптографические шифры за день, а не за миллионы лет, которые нужны классическим компьютерам на аналогичные задачи.

В связке с квантовыми коммуникациями развиваются решения информационной безопасности на основе квантово-устойчивых алгоритмов шифрования (постквантовая криптография).

Постквантовая криптография — это новое поколение криптографических алгоритмов, которые оказываются устойчивыми как к атакам с применением традиционных вычислительных архитектур, так и к атакам с применением квантовых компьютеров.

По сравнению с традиционными алгоритмами, постквантовые используют другие математические принципы. Квантовая и постквантовая криптографии дополняют друг друга, как аппаратные и программные решения в классической криптографии. Если посмотреть, как это применяется на практике, мы увидим, что квантовая криптография подходит для защиты высоконагруженных каналов связи и каналов, по которым передается стратегически ценная информация. Например, между банковскими офисами, дата-центрами или видеоконференции топ-менеджмента. В это же время постквантовая криптография может решить задачи по безопасности ненагруженных каналов.

Например, южнокорейский мобильный оператор LGU+ интегрировал постквантовую технологию в свое сетевое оборудование. При этом компания

отмечает, что решение актуально для проводных коммуникаций, беспроводных сетей и 5G. О разработке нескольких квантово-безопасных проектов также заявили представители IBM. В области развития постквантовой криптографии QRate работает совместно с проектом QApp Российского квантового центра.

Связь с космосом

Наземные и подземные телекоммуникационные системы имеют ограничения по покрытию. Во многих местах нашей планеты проложить такие сети невозможно. Поэтому еще один вызов квантовой эры — научиться осуществлять передачу сигнала квантовым методом через спутник.

Летом 2020 года был установлен рекорд дальности передачи зашифрованного сообщения без промежуточных точек приема-передачи. Ученые Китая использовали запутанные фотоны со спутника квантовой связи. Две обсерватории в Китае, которые отправляли и принимали сообщения, были удалены друг от друга 1200 километров. При этом при передаче сигнала был отмечен очень низкий коэффициент ошибок. Это имеет важное значение для создания безопасного интернета. В случае перехвата сигнала злоумышленниками точка приема на Земле обнаружит резкий скачок уровня ошибок в передаваемом ключе. И его просто не будут использовать для расшифровки информации. Поэтому уровень базовых ошибок должен быть как можно более низким. Достижения в этой области помогут увеличить зону покрытия квантово-безопасной передачи данных.

Как защититься от атак

Может показаться, что все эти векторы страшно далеки от реальности, но посмотрев на кейсы 2020 года, можно отметить, что индустрия ждет первого публичного случая взлома с применением квантового компьютера. После этого ландшафт кибербезопасности серьезно изменится. Наличие возможности взлома, скорее всего, будет известно широкой публике не сразу. Идти в квантовую эру нужно спокойными и последовательными шагами.

Этап 1: проверить, что ваш отдел информационной безопасности знает о новых технологиях и методах защиты данных. Если знаний недостаточно, то принять участие в открытых образовательных мероприятиях по квантовым технологиям, которые регулярно проводят ведущие технологические вузы страны, например, МИСиС.

Этап 2: проанализировать ценность данных в своей организации. Квантовая криптография в первую очередь потребуется тем компаниям, которые передают или обрабатывают критически важную информацию и персональные данные пользователей с длительным периодом хранения. Например, в телекоммуникационной, банковской и IT-отраслях. Подобный анализ уже доступен в индустрии, а не только в научных лабораториях.

Этап 3: разработать новую стратегию информационной безопасности и определить необходимый объем инвестиций. Отталкиваясь от этого, подобрать и изучить решения, которые помогут вашему бизнесу перейти на квантово-безопасную архитектуру. На этом этапе для каждой компании нужен индивидуальный подход, основанный на действующем уровне подготовки персонала и технического оснащения.

Этап 4: развивать новые технологические компетенции внутри своей компании, нанимать специалистов, понимающих квантовые коммуникации или обучать профильных сотрудников заранее. Квантовые коммуникации — это новая отрасль в контексте коммерциализации технологии. Еще недавно она была закрыта в лабораториях, а сегодня уже рынок формирует постоянный запрос на специалистов в этой области. Например, JPMorgan реализуют общую стратегию, направленную одновременно на квантовые вычисления и квантовые коммуникации. Недавно компания опубликовала вакансии, которые показывают ее интерес к разработке квантовых алгоритмов, применяемых к искусственному интеллекту, оптимизации и криптографии.

Этап 5: как и в случае любой другой потенциальной угрозы, не ждать «последнего момента», а запланировать переход на квантово-защищенные решения в циклах обновления информационной инфраструктуры при сотрудничестве экспертов в области интеграции квантовых коммуникаций». ***(Юрий Курочкин. Берегите данные: как защититься от атак с применением квантового компьютера уже сегодня // ООО "РБ.РУ" (https://rb.ru/opinion/quantum-cybersecurity/). 26.01.2021).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Nvidia выпустила ряд исправлений безопасности, решающих серьезные проблемы в драйвере дисплея графического процессора Nvidia и программном обеспечении vGPU.

Выпущенные в четверг технологический гигант заявил, что исправления решают проблемы, которые «могут привести к отказу в обслуживании, повышению привилегий, подделке данных или раскрытию информации».

В общей сложности Nvidia устранила 16 уязвимостей, связанных с драйвером дисплея графического процессора Nvidia, который используется для поддержки графических процессоров, а также в программном обеспечении vGPU для виртуальных рабочих станций, серверов, приложений и ПК.

Самая серьезная уязвимость, с которой столкнулись в последнем раунде безопасности Nvidia, - это CVE - 2021-1051. Полученная оценка CVSS 8,4, проблема затрагивает уровень режима ядра для драйвера дисплея графического процессора Windows. В случае использования этот недостаток может привести к отказу в обслуживании или повышению привилегий.

CVE - 2021-1052 - вторая по значимости уязвимость в драйвере, но эта ошибка затрагивает как Windows, так и Linux. Недостаток безопасности, которому присвоена оценка серьезности 7,8, также обнаружен на уровне режима ядра и позволяет клиентам пользовательского режима получать доступ к устаревшим привилегированным API. В результате эксплойт, использующий эту уязвимость,

может привести к отказу в обслуживании, повышению привилегий и утечке информации.

Nvidia также устранила CVE - 2021-1053, ошибку драйвера дисплея для компьютеров Windows и Linux с оценкой CVSS 6,6, что указывает на то, что эта уязвимость считается умеренной / важной проблемой. Неправильная проверка указателя пользователя, нацеленного на тот же уровень режима ядра, может привести к отказу в обслуживании.

Две другие проблемы влияют на компьютеры Windows в том же уровне режима ядра, которые отслеживаются как CVE - 2021-1054 и CVE - 2021-1055 с оценками серьезности 6.5 и 5.3 соответственно. Эти уязвимости включают в себя сбои при проверке авторизации и неправильный контроль доступа, и их можно использовать для отказа в обслуживании. CVE - 2021-1055 также может привести к утечке данных.

Последняя уязвимость затрагивает только ПК с ОС Linux. Эта ошибка, отслеживаемая как CVE - 2021-1056 и получившая оценку CVSS 5,3, была вызвана ошибками разрешений файловой системы операционной системы, вызывающими раскрытие информации и отказ в обслуживании.

В общей сложности 10 уязвимостей, о которых сообщалось, затрагивают vGPU Nvidia, восемь из которых относятся к диспетчеру vGPU.

За исключением CVE - 2021-1066, умеренной проблемы проверки ввода CVSS 5.5 в диспетчере vGPU, приводящей к перегрузке ресурсов и отказу в обслуживании, каждой уязвимости была присвоена оценка серьезности 7,8.

Nvidia устранила восемь уязвимостей диспетчера vGPU и плагинов, начиная от ошибок проверки входных данных и заканчивая условиями гонки и ненадежными исходными значениями. Эти недостатки безопасности могут привести к раскрытию информации, потере целостности и конфиденциальности и фальсификации данных.

Две уязвимости проверки входного индекса, CVE - 2021-1058 и CVE - 2021-1060, влияют на драйвер режима гостевого ядра и подключаемый модуль vGPU. Первый может быть вызван целочисленным переполнением, допускающим подделку данных, утечку данных и отказ в обслуживании, тогда как второй может быть использован для отказа в обслуживании и манипулирования данными.

Чтобы оставаться в безопасности, Nvidia рекомендует пользователям принимать автоматические обновления безопасности или загружать их напрямую». ***(Charlie Osborne. Nvidia releases security update for high-severity graphics driver vulnerabilities // ZDNet (https://www.zdnet.com/article/nvidia-releases-security-update-for-high-severity-graphics-driver-vulnerabilities/). 08.01.2021).***

***

«Основные браузеры получают обновление для исправления отдельных ошибок, которые допускают удаленные атаки, что потенциально может позволить хакерам захватить целевые устройства.

Создатели браузеров Chrome, Firefox и Edge призывают пользователей исправлять критические уязвимости, которые в случае эксплуатации позволяют хакерам взламывать системы, на которых запущено программное обеспечение.

Уязвимость Mozilla Firefox (CVE-2020-16044) отличается от ошибки, обнаруженной в движке браузера Google Chromium, который используется в браузере Google Chrome и последней версии браузера Edge от Microsoft.

Критическая ошибка использования Firefox после освобождения

В четверг Агентство по кибербезопасности и безопасности инфраструктуры (CISA) призвало пользователей браузера Mozilla Foundation Firefox исправить ошибку, отмеченную как CVE-2020-16044 и оцененную как критическую. Уязвимость классифицируется как ошибка использования после освобождения и связана с тем, как Firefox обрабатывает файлы cookie браузера, и в случае использования позволяет хакерам получить доступ к компьютеру, телефону или планшету, на котором запущено программное обеспечение браузера.

Это затронуло версии браузера Firefox, выпущенные до недавно выпущенного Firefox Desktop 84.0.2, Firefox Android 84.1.3 edition, а также корпоративную версию Firefox ESR 78.6.1 от Mozilla.

«Злоумышленник мог изменить фрагмент COOKIE-ECHO в пакете SCTP таким образом, чтобы потенциально привести к использованию после освобождения. Мы предполагаем, что при достаточных усилиях он мог быть использован для запуска произвольного кода», - говорится в бюллетене по безопасности Mozilla, опубликованном в четверг.

Аббревиатура SCTP означает протокол передачи управления потоком, используемый в компьютерных сетях для передачи данных протокола на транспортном уровне набора интернет-протоколов или TCP / IP. Ошибка связана со способом обработки данных файлов cookie с помощью SCTP.

Каждый входящий пакет SCTP содержит фрагмент cookie, который обеспечивает соответствующий ответ от cookie браузера. Блок COOKIE ECHO - это фрагмент данных, отправленный во время инициализации соединения SCTP с браузером.

Согласно Mozilla, злоумышленник может создать вредоносный блок COOKIE-ECHO, чтобы повлиять на память браузера. Уязвимость использования после освобождения связана с некорректным использованием динамической памяти во время работы программы. Если после освобождения области памяти программа не очищает указатель на эту память, злоумышленник может использовать ошибку для взлома программы», - говорится в описании уязвимости.

Mozilla не поверила в обнаружение ошибки и не указала, была ли эта уязвимость активно эксплуатируемой в дикой природе.

Ошибка браузера Chromium влияет на Chrome и Edge

Также в четверг CISA призвал пользователей Windows, macOS и Linux браузера Chrome от Google исправить ошибку записи за пределами допустимого диапазона (CVE-2020-15995), влияющую на текущую версию программного обеспечения 87.0.4280.141. В предупреждении об ошибке CISA говорилось, что обновление до последней версии браузера Chrome «устранит уязвимости, которые злоумышленник может использовать, чтобы получить контроль над уязвимой системой».

Поскольку последний браузер Microsoft Edge основан на движке браузера Google Chromium, Microsoft также призвала своих пользователей обновить браузер Edge до последней версии 87.0.664.75.

В то время как исследователи из Tenable классифицируют ошибку, выходящую за пределы допустимого диапазона, как критическую, и Google, и Microsoft классифицируют уязвимость как высокую. Исследователю Tencent Security Xuanwu Lab Бохану Лю приписывают обнаружение и сообщение об ошибке.

Интересно, что ошибка CVE-2020-15995 восходит к бюллетеню по безопасности обновления Chrome для Android, который Google опубликовал в октябре 2020 года. В то время ошибка также была классифицирована как серьезная. Недостаток определяется как «запись вне пределов V8», ошибка, первоначально обнаруженная Лю в сентябре 2020 года.

Согласно описанию разработчика Google, V8 - это высокопроизводительный движок JavaScript и WebAssembly с открытым исходным кодом от Google. Хотя техническая специфика ошибки недоступна, аналогичные записи за пределами допустимого диапазона ошибок V8 позволили удаленным злоумышленникам использовать повреждение кучи с помощью созданной HTML-страницы.

Повреждение кучи - это тип повреждения памяти, который происходит в компьютерной программе, когда содержимое области памяти изменяется из-за программного поведения - злонамеренного или нет - которое выходит за рамки намерений исходного программиста или параметров языка программы. Согласно академической статье (PDF), в соавторстве с Нектариосом Георгиосом Цуцосом, членом-студентом IEEE, и Михаилом Маниатакосом, старшим членом IEEE, может использоваться так называемая атака с разрушением кучи.

«Атаки с разбиванием кучи используют средства распределения динамической памяти (например, malloc), повреждая структуры управления, определяющие саму кучу. Переполняя блок кучи, злоумышленники могут перезаписывать соседние заголовки кучи, которые связывают разные блоки кучи, и в конечном итоге заставляют распределитель динамической памяти изменять произвольные ячейки памяти, как только выполняется операция освобождения кучи. Вредоносная полезная нагрузка также может быть сгенерирована на лету: например, используя JIT-компиляцию, собранный код можно записать в куче», - написали они.

Ни Microsoft, ни Google не объясняют, почему октябрьский 2020 года CVE-2020-15995 снова появляется в обоих бюллетенях по безопасности за четверг. Обычно это признак того, что исходное исправление было неполным.

Другие ошибки Chromium влияют на Chrome и Edge

Google сообщил о двенадцати дополнительных ошибках, влияющих на его браузерную систему Chromium. И у Google, и у Microsoft был один и тот же список уязвимостей (CVE-2021-21106, CVE-2021-21107, CVE-2021-21108, CVE-2021-21109, CVE-2021-21110, CVE-2021-21111, CVE-2021. -21112, CVE-2021-21113, CVE-2021-21114, CVE-2021-21115, CVE-2021-21116, CVE-2020-16043).

Большинство ошибок имели высокий уровень серьезности и были связаны с ошибками использования после исправления. Три уязвимости принесли охотникам

за ошибками 20 000 долларов за свои усилия. Вэйпэн Цзян из Codesafe Team Legendsec в Qi'anxin Group признан за обнаружение ошибок на сумму 20 000 долларов (CVE-2021-21106 и CVE-2021-21107). Первая - ошибка использования после освобождения, связанная с функцией автозаполнения Chromium, а вторая - ошибка использования после освобождения в медиа-компоненте Chromium.

Ликрасо и Гуан Гонг из 360 Alpha Lab заработали 20 000 долларов за CVE-2021-21108, также являющуюся ошибкой использования после бесплатного использования в медиа-компоненте браузера.

Никаких технических подробностей не разглашается, и обычно это происходит до тех пор, пока не будет установлено, что большинство браузеров Chrome было обновлено». ***(Tom Spring. Bugs in Firefox, Chrome, Edge Allow Remote System Hijacking // Threatpost (https://threatpost.com/firefox-chrome-edge-bugs-system-hijacking/162873/). 08.01.2021).***

***

«Производитель сетевого оборудования Cisco вчера заявила, что не собирается выпускать обновления прошивки для исправления 74 уязвимостей, о которых сообщалось в его линейке маршрутизаторов RV, срок службы которых подошел к концу (EOL).

Затронутые устройства включают системы Cisco Small Business RV110W, RV130, RV130W и RV215W, которые можно использовать как в качестве маршрутизаторов, так и в качестве межсетевых экранов и сетей VPN.

Все четыре достигли EOL в 2017 и 2018 годах, а также недавно вышли из своего последнего окна обслуживания в рамках контрактов на платную поддержку 1 декабря 2020 года.

В трех рекомендациях по безопасности, опубликованных вчера [1, 2, 3], Cisco сообщила, что с декабря она получает отчеты об ошибках для уязвимостей, начиная от простого отказа в обслуживании, приводящего к сбою устройств, до недостатков безопасности, которые можно использовать для получения доступа к учетным записям root и угонить роутеры.

В общей сложности производитель устройств заявил, что получил 74 отчета об ошибках, но не будет выпускать какие-либо программные исправления, средства защиты или обходные пути, поскольку устройства уже давно достигли EOL годами ранее.

Вместо этого компания посоветовала клиентам перенести операции на новые устройства, такие как модели RV132W, RV160 или RV160W, которые обеспечивают те же функции и все еще активно поддерживаются.

Некоторым клиентам компании может не понравиться решение компании, но хорошая новость заключается в том, что ни одна из обнаруженных сегодня ошибок не может быть легко использована.

Cisco заявила, что все уязвимости требуют, чтобы у злоумышленника были учетные данные для устройства, что снижает риск атаки на сеть в ближайшие недели или месяцы, давая администраторам возможность спланировать и подготовить план перехода на новое оборудование или, по крайней мере, в противном случае применить свои собственные контрмеры…» ***(Catalin Cimpanu.***

Cisco says it won't patch 74 security bugs in older RV routers that reached EOL // ZDNet (https://www.zdnet.com/article/cisco-says-it-wont-patch-74-security-bugs-in-older-rv-routers-that-reached-eol/). 14.01.2021).

***

«Неизвестная уязвимость межсайтового скриптинга (XSS) в Apache Velocity Tools может быть использована неаутентифицированными злоумышленниками для нацеливания на правительственные сайты, включая НАСА…

Apache Velocity - это механизм шаблонов на основе Java, используемый разработчиками для проектирования представлений в архитектуре модель-представление-контроллер (MVC).

Velocity Tools - это подпроект, включающий классы, которые еще больше упрощают интеграцию Velocity в стандартные и веб-приложения.

Правительственные сайты, использующие Apache Velocity Tools, уязвимы для XSS

Apache Velocity Tools имеет нераскрытую XSS-уязвимость, которая затрагивает все его версии, несмотря на то, что исправление было опубликовано на GitHub несколько месяцев назад.

Хотя официального раскрытия уязвимости не произошло, BleepingComputer был проинформирован о том, что эта уязвимость отслеживается внутри компании как CVE-2020-13959.

При запросе систем Nexus Intelligence от Sonatype я обнаружил, что класс Apache Velocity Tools, содержащий этот недостаток, включен в более чем 2600 уникальных двоичных файлов известных программных приложений, доступных для загрузки из npm, PyPI, Maven Central и других репозиториев с открытым исходным кодом.

Популярность компонента среди разработчиков делает критически важным своевременное раскрытие уязвимостей, влияющих на Velocity Tools.

Исследователь безопасности Джексон Генри из этической хакерской группы Sakura Samurai впервые обнаружил уязвимость Apache и сообщил о ней в начале октября 2020 года.

Хотя проект признал отчет Генри и опубликовал общедоступное исправление на GitHub 5 ноября 2020 года, надлежащего публичного раскрытия так и не произошло, что обеспокоило исследователей Sakura Samurai.

Отраженный недостаток XSS существует в том, как класс представления VelocityViewServlet отображает страницы ошибок.

Когда недействительный URL доступен, то «шаблон не найден» ошибка страница отражает путь часть ресурсов в URL, как это, не избежать его возможных сценариев XSS.

Следовательно, злоумышленник может обманом заставить жертву щелкнуть такой URL-адрес, который приведет жертву на измененную фишинговую страницу или извлечет информацию о сеансе входа в систему.

По наблюдениям BleepingComputer, уязвимые экземпляры Apache Velocity Tools используются правительственными веб-сайтами, включая * .nasa.gov и * .gov.au.

Более сложные варианты этого XSS-эксплойта в сочетании с некоторыми приемами социальной инженерии могут позволить злоумышленникам собирать файлы cookie сеансов вошедших в систему пользователей и потенциально перехватывать их сеансы.

Это особенно актуально для порталов входа в систему для сотрудников и подрядчиков, размещенных на государственных доменах...

Apache: отчеты об уязвимостях с сортировкой по степени серьезности

Когда BleepingComputer обратился за комментариями, представители Apache Software Foundation (ASF) заявили, что группа безопасности Apache получает сотни отчетов об уязвимостях в год и что они своевременно реагируют на них в зависимости от серьезности проблемы, как показано в их годовой отчет о безопасности.

«Что касается XSS-уязвимости в инструментах Apache Velocity, 6 октября 2020 года с группой безопасности Apache впервые связался человек (называемый докладчиком о проблеме), который сообщил о проблеме, которая, как они обнаружили, затрагивает часть пакета Velocity Tools».

«Мы поделились этим в частном порядке с Комитетом управления проектами Apache Velocity Project Management (PMC), который провел расследование и принял отчет 7 октября и предложил репортеру представить исправление».

"Затем репортер отправил запрос на перенос, и в течение нескольких недель команда работала над уточнением исправления. Это исправление было применено 5 ноября. Репортер представил свой патч публично 8 октября и из-за отсутствия критический характер уязвимости, команда Velocity решила продолжить работу над проблемой публично».

«Этот вопрос был внутренне назначен CVE-2020-13959 8 октября,» сказал Марк J Кокс, вице - президент ASF безопасности BleepingComputer в заявлении.

Следующим шагом, оставшимся для проекта, является создание фиксированного выпуска Velocity Tools, в котором будет упоминаться CVE и путь обновления, дата которого еще не определена.

Однако пользователи, которые предпочли бы не дожидаться выпуска исправления, могут сами поэкспериментировать с применением общедоступного исправления.

Растущее беспокойство по поводу поставщиков, выступающих в роли CNA

В последнее время, когда количество отчетов об уязвимостях продолжает расти экспоненциально, MITER, некоммерческая организация, которой поручено назначать идентификаторы CVE, столкнулась с проблемами масштабируемости.

Чтобы ускорить процесс присвоения CVE и ответственного раскрытия информации, была введена концепция органов нумерации CVE (CNA).

Организации, получившие одобрение в качестве CNA, уполномочены назначать CVE для отчетов об уязвимостях и обрабатывать ответственный процесс раскрытия информации от имени MITRE.

Однако в последнее время все больше и больше поставщиков стремятся стать CNA и взять под контроль процесс раскрытия уязвимостей.

Это заставило профессионалов в области информационной безопасности опасаться, может ли такое развитие событий действительно снизить безопасность в долгосрочной перспективе.

Как ранее сообщалось на The Daily Swig, в соответствии с правилами митре, в КНО не требуется, чтобы назначить CVEs к уязвимости сообщалось в частном порядке на проекты, некоторые из которых могут включать свои собственные продукты.

Это означает, что поставщики могут спокойно исправлять даже самые серьезные проблемы с безопасностью прямо сейчас, без необходимости немедленно сообщать о них публично.

Совсем недавно это произошло в случае VMWare, когда исследователи PT Swarm сообщили об уязвимости чтения файлов без аутентификации в vCenter, которая была незаметно исправлена VMWare без немедленной выдачи CVE.

«Компаниям необходимо серьезно относиться к уязвимостям безопасности и работать с исследователями над разработкой исправлений».

«Связь и обновления статуса имеют важное значение для того, чтобы держать исследователей в курсе, это важный аспект исправления, который можно упустить из виду и нанести ущерб прозрачности - даже обескураживающий», - сказал Генри BleepingComputer в интервью по электронной почте.

Команда безопасности Apache поделилась деталями своего процесса обработки CVE с BleepingComputer, который иногда может включать в себя кратковременную задержку раскрытия уязвимостей для некритических проблем.

«Если вопросы безопасности не являются критическими, некоторые проекты откладывают выпуск релиза на короткое время, чтобы одновременно решить другие проблемы».

"Следует отметить, что в этом случае на каждое электронное письмо, которое репортер проблемы отправил в группу безопасности ASF, был дан ответ в течение одного рабочего дня, причем репортер хвалил наш быстрый ответ, поэтому мы немного удивлены, узнав, что репортер считает, что они ", - сообщили BleepingComputer команда безопасности Apache». ***(Ax Sharma. Undisclosed Apache Velocity XSS vulnerability impacts GOV sites // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/undisclosed-apache-velocity-xss-vulnerability-impacts-gov-sites/). 15.01.2021).***

***

«Онлайн-опросы и программное обеспечение для создания форм как услуга Typeform устранила уязвимость, связанную с перехватом информации.

Недостаток, который существовал в интеграции приложения Typeform с Zendesk Sell, мог позволить злоумышленникам незаметно перенаправлять отправленные формы с потенциально конфиденциальными данными на себя.

Идентификаторы форм Typeform, проиндексированные поисковыми системами

Инструмент для онлайн-опросов и создания форм Typeform позволяет пользователям создавать веб-страницы для удобного сбора данных от пользователей.

Каждая такая форма, созданная на платформе, имеет уникальный «идентификатор формы», например, hHXhmf, который в случае общедоступных опросов может быть проиндексирован поисковыми системами, как это обнаруживает BleepingComputer.

За кулисами системы Typeform используют этот идентификатор формы во всех рабочих процессах, чтобы отслеживать отправку форм и передавать собранные данные между различными частями приложения.

При нормальных обстоятельствах знание этого идентификатора формы просто позволит любому пользователю получить доступ и заполнить соответствующий опрос.

Однако серьезная уязвимость в Typeform означала, что злоумышленники могли скрытно собирать ответы, отправленные респондентами, практически для любой формы, если они знали этот идентификатор.

Нарушенная интеграция с Zendesk позволяет злоумышленникам захватывать отправленные материалы

Не называя явно Typeform, охотник за головами Ронак Патель недавно предоставил подробности об ошибке, связанной с небезопасной прямой ссылкой на объект (IDOR), которая повлияла на «приложение [используемое] для создания форм для опросов, викторин и прочего».

В ходе дальнейшего расследования BleepingComputer обнаружил, что недостаток существовал в Typeform.

Уязвимости IDOR возникают, когда к системному объекту, имеющему ссылку, могут получить несанкционированный доступ напрямую пользователи.

В этом случае объект относится к форме / опросу Typeform, а ссылкой является «form_id», который может позволить злоумышленникам подключиться к данным, отправленным для формы.

Typeform позволяет интегрировать приложения и веб-сервисы, такие как Google Analytics и Zendesk Sell, чтобы улучшить обработку отправки форм.

Например, создатели опросов могут использовать приложение Zendesk Sell и сопоставить поля ответов на опрос с полями Zendesk Sell в своей учетной записи для анализа данных.

Zendesk Sell - это CRM-система продаж и программное обеспечение для преобразования потенциальных клиентов, которое объясняет, почему создатели опросов Typeform из определенных областей бизнеса могут найти его полезным.

Пател создал тестовую учетную запись Zendesk Sell и интегрировал ее со своей учетной записью Typeform.

Он наблюдал, как сетевые запросы, включая поля GET и POST, обмениваются между Typeform и Zendesk Sell на протяжении всего рабочего процесса интеграции.

Его внимание привлекло поле form_id…

Исследователь дополнительно создал «взломщик» Sell счет Zendesk для тестирования и заметил, что это можно было подделать поле «form_id» передаются

в запросе интеграции на произвольное значение, например, как form_id обследования Typeform, принадлежащих потерпевшему.

Это означает, что злоумышленники могут случайно продолжить поиск идентификаторов форм Typeform, которые время от времени индексируются поисковыми системами.

Но сейчас. Используя этот недостаток интеграции приложения, участники могли собирать собранные ответы на опрос в своих учетных записях Zendesk Sell, при этом создатель опроса не знал о происходящей незаконной деятельности.

«Подводя итог, используя IDOR в этом процессе интеграции, злоумышленник может интегрировать свою учетную запись для продажи Zendesk с любой формой без какого-либо взаимодействия с пользователем и может получить все конфиденциальные данные, полученные в виде ответа на форму», - сказал Патель.

Патель утверждает, что уязвимость была обнаружена им около шести месяцев назад и исправлена платформой два месяца назад…». ***(Ax Sharma. Typeform fixes Zendesk Sell form data hijacking vulnerability // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/typeform-fixes-zendesk-sell-form-data-hijacking-vulnerability/). 11.01.2021).***

***

«Сегодня исследователи ответственно раскрыли уязвимость системы безопасности, воспользовавшись которой, они могли получить доступ к записям более 100 000 частных сотрудников Программы Организации Объединенных Наций по окружающей среде (ЮНЕП).

Нарушение данных произошло из-за открытых каталогов и учетных данных Git, что позволило исследователям клонировать репозитории Git и собрать большой объем личной информации (PII), связанной с сотрудниками ЮНЕП.

Каталог Git предоставил базу данных WordPress и учетные данные Git

Группа исследователей этического взлома и безопасности Sakura Samurai раскрыла свои выводы об уязвимости, которая позволила им получить доступ к более чем 100 000 личных записей сотрудников Программы Организации Объединенных Наций по окружающей среде (ЮНЕП).

Документы и снимки экрана, предоставленные BleepingComputer, содержат подробные сведения о природе этой уязвимости безопасности и обо всем, что она обнаружила.

Наткнувшись на Программу раскрытия уязвимостей Организации Объединенных Наций и Зал славы InfoSec, исследователи Джексон Генри, Ник Салер, Джон Джексон и Обри Коттл из Sakura Samurai приступили к поиску любых недостатков безопасности, влияющих на системы ООН.

Затем они обнаружили открытые каталоги Git (.git) и файлы учетных данных Git (.git-credentials) в доменах, связанных с ЮНЕП и Международной организацией труда (МОТ) Организации Объединенных Наций.

Исследователи смогли сбросить содержимое этих файлов Git и клонировать целые репозитории из доменов * .ilo.org и * .unep.org с помощью git-dumper.

В .git содержимого каталога включают важные файлы, такие как WordPress файлы конфигурации (WP-config.php) разоблачающих учетные данные базы данных администратора.

Аналогичным образом, различные файлы PHP, раскрытые как часть этой утечки данных, содержали учетные данные базы данных в открытом виде, связанные с другими онлайн-системами ЮНЕП и МОТ ООН.

Кроме того, общедоступные файлы .git-credentials позволили исследователям получить доступ к базе исходного кода ЮНЕП.

Извлеченные данные содержат более 100 000 записей о сотрудниках

Используя эти учетные данные, исследователи смогли изъять более 100 000 записей сотрудников ООН из различных систем.

Набор данных, полученных группой, показал историю поездок сотрудников ООН, каждая строка которой содержит: идентификатор сотрудника, имена, группы сотрудников, обоснование командировки, даты начала и окончания, статус утверждения, пункт назначения и продолжительность пребывания.

Аналогичным образом, в других базах данных ООН, к которым исследователи обращались в рамках своего анализа, были представлены демографические данные HR (национальность, пол, уровень оплаты труда) по тысячам сотрудников, записи источников финансирования проектов, обобщенные записи сотрудников и отчеты об оценке занятости.

В интервью по электронной почте BleepingComputer группа сказала:

«Когда мы начали исследовать ООН, мы не думали, что это разовьется так быстро. В течение нескольких часов у нас уже были конфиденциальные данные и выявлены уязвимости. В целом, менее чем за 24 часа мы получили все эти данные», - Сакура Самурай сказал BleepingComputer.

«В общей сложности мы нашли 7 дополнительных пар учетных данных, которые могли привести к несанкционированному доступу к нескольким базам данных. Мы решили остановить и сообщить об этой уязвимости, как только мы смогли получить доступ к PII, которая была раскрыта через резервные копии баз данных, которые были в частных проектах, "заявляют исследователи в своем блоге.

Скорее всего, злоумышленники уже получили доступ к данным

Исследователи поделились с BleepingComputer серией электронных писем, в которых было показано, что они изначально сообщили ООН об уязвимости в частном порядке 4 января 2021 года.

Управление ООН по информационным и коммуникационным технологиям (OICT) первоначально признало их отчет, но, не осознавая уязвимости ЮНЕП, ответило:

«Сообщенная уязвимость не относится к Секретариату Организации Объединенных Наций, а относится к МОТ (Международной организации труда)», - говорится в электронных письмах, увиденных BleepingComputer, и чем-то, что ООН, как известно, делала в прошлом.

В конце концов, согласно этим электронным письмам, Сайфул Ридван, руководитель отдела корпоративных решений в ЮНЕП, поблагодарил исследователей за их отчет об уязвимости, заявив, что их команда DevOps

предприняла немедленные шаги по исправлению уязвимости и что оценка воздействия этой уязвимости находится в процессе.

Кроме того, в последующем электронном письме для исследователей, просмотренном BleepingComputer, ЮНЕП заявила, что уведомление о разглашении данных находится в разработке, но это «сложно, поскольку мы не делали этого раньше».

В целом, как сообщили BleepingComputer исследователи, Организация Объединенных Наций быстро исправила эту проблему безопасности менее чем за неделю.

«Честно говоря, я благодарен Сайфулу за быстрые исправления. Несмотря на то, что он заявил, что это было для него довольно ново, они установили исправления с рекордной скоростью и защитили данные».

«На данный момент наша единственная забота - проинформировать затронутых пользователей. В частности, Обри Коттл, также известный как Киртанер, отметил, что, если бы было так легко получить данные, злоумышленники, вероятно, уже имеют данные».

«Группа согласилась с тем, что ЮНЕП должна проанализировать траекторию раскрытого PII, чтобы определить, сколько субъектов угрозы, если таковые имеются, имеют данные», - сказал BleepingComputer основатель Sakura Samurai Джон Джексон.

Это не первый случай утечки данных в системы ООН.

В 2019 году ООН не раскрыла информацию о кибератаке, которая серьезно повредила их сети и базы данных.

В 2020 году ООН наконец обнародовала информацию, в которой вину за взлом возложили на уязвимость SharePoint.

ЮНЕП: никаких признаков дополнительного несанкционированного доступа

BleepingComputer обратилась в ЮНЕП за комментариями, и сначала нам сказали: «Спасибо, что сообщили нам об этой проблеме. Мы связываемся с нашими экспертами и коллегами, и мы вернемся, как только у нас будет соответствующая информация».

15 января 2021 года представитель ЮНЕП поделился с BleepingComputer дополнительной информацией:

«После уведомления о взломе 4 января 2021 года уязвимость была устранена в течение 12 часов. Взломанные данные включают более 100 000 строк информации, включая данные о кадрах и поездках за период с 2015 по 2018 годы».

«ЮНЕП не известно ни о дополнительном несанкционированном доступе к информации, ни о каком-либо неправомерном использовании данных. Набор данных не содержит информации, которая может быть использована для атаки на любые другие данные ООН или ИТ-системы».

"Об этом нарушении было сообщено в Организацию Объединенных Наций через созданную программу этического взлома " Зала славы информационной безопасности». Эта программа позволяет общественности оказывать помощь в защите ИКТ-ресурсов путем обнаружения и раскрытия уязвимостей в общедоступной информационной системе ООН. "

«ЮНЕП работает с экспертами Секретариата ООН по кибербезопасности, чтобы устранить утечку данных и укрепить свою ИТ-безопасность», - сказал BleepingComputer представитель ЮНЕП». ***(Ax Sharma. United Nations data breach exposed over 100k UNEP staff records // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/united-nations-data-breach-exposed-over-100k-unep-staff-records/). 11.01.2021).***

***

«Две уязвимости безопасности - одна проблема повышения привилегий, а другая - сохраненная ошибка XSS - поражают плагин WordPress с 40 000 установками.

Две уязвимости (одна критическая) в плагине WordPress под названием Orbit Fox могут позволить злоумышленникам внедрить вредоносный код в уязвимые веб-сайты и / или получить контроль над веб-сайтом.

Orbit Fox - это многофункциональный плагин WordPress, который работает с утилитами для создания сайтов Elementor, Beaver Builder и Gutenberg. Он позволяет администраторам сайта добавлять такие функции, как регистрационные формы и виджеты. Плагин от разработчика ThemeIsle был установлен более чем на 400 000 сайтов.

По мнению исследователей Wordfence, первый недостаток (CVE ожидает рассмотрения) - это недостаток аутентифицированного повышения привилегий, который имеет оценку серьезности ошибки CVSS 9,9, что делает его критическим. Злоумышленники, прошедшие проверку подлинности с доступом на уровне участника или выше, могут повысить себя до статуса администратора и потенциально захватить сайт WordPress.

Вторая ошибка - это проблема аутентифицированного хранимого межсайтового скриптинга (XSS), которая позволяет злоумышленникам с доступом на уровне участника или автора внедрять JavaScript в сообщения. Эту инъекцию можно использовать, среди прочего, для перенаправления посетителей на сайты с вредоносной рекламой или создания новых административных пользователей. Он получил оценку 6,4 по шкале CVSS, что делает его средней степенью серьезности.

Повышение привилегий

По словам исследователей, ошибка повышения привилегий существует в виджете регистрации Orbit Fox.

Виджет используется для создания регистрационных форм с настраиваемыми полями при использовании плагинов для построения страниц Elementor и Beaver Builder. Администраторы сайта могут установить роль по умолчанию, которая будет назначаться пользователям, которые регистрируются на сайте с помощью формы.

«Пользователям более низкого уровня, таким как участники, авторы и редакторы, не была показана возможность установить роль пользователя по умолчанию из редактора. Однако мы обнаружили, что они все еще могут изменять роль пользователя по умолчанию, создавая запрос с соответствующим параметром», - пояснили исследователи Wordfence во вторник. «Плагин обеспечивал защиту на стороне клиента, чтобы предотвратить отображение

селектора ролей для пользователей нижнего уровня при добавлении формы регистрации. К сожалению, не было никакой защиты или проверки на стороне сервера, чтобы убедиться, что авторизованный пользователь действительно устанавливал роль пользователя по умолчанию в запросе».

Проверка на стороне сервера происходит, когда данные отправляются на сервер, когда пользователь вводит их в форму. После того, как сервер получит запрос, он проверит наличие проблем с безопасностью, обеспечит правильный формат данных и подготовит отправку для вставки или обновления в источник данных.

Отсутствие проверки на стороне сервера в Orbit Fox означает, что участники, авторы и редакторы более низкого уровня для сайта могут установить роль пользователя в роли администратора после успешной регистрации, поэтому все, что нужно будет сделать злоумышленникам, - это зарегистрироваться как новые. пользователей, а затем получит права администратора.

«Чтобы воспользоваться этой уязвимостью, необходимо включить регистрацию пользователей и на сайте должны быть запущены плагины Elementor или Beaver Builder», - говорит Wordfence. «Сайт с отключенной регистрацией пользователей или ни один из этих плагинов не будет подвержен этой уязвимости».

Сохраненный XSS

По словам Wordfence, проблема средней степени серьезности возникает из-за того, что участники и авторы могут добавлять сценарии к сообщениям, несмотря на то, что у них нет возможности uniltered_html из-за функции сценариев верхнего и нижнего колонтитула в Orbit Fox.

«Этот недостаток позволял пользователям более низкого уровня добавлять вредоносный JavaScript в сообщения, которые выполнялись в браузере всякий раз, когда пользователь переходил на эту страницу», - пояснили исследователи. «Как всегда в случае с XSS-уязвимостями, это позволит злоумышленникам создать новых административных пользователей, внедрить вредоносные перенаправления и бэкдоры или изменить другой контент сайта с помощью вредоносного JavaScript».

Обе проблемы исправлены в версии 2.10.3; те сайты, на которых установлена версия Orbit Fox 2.10.2 и ниже, должны обновиться как можно скорее.

Проблемы с плагином WordPress

Ошибки Orbit Fox являются последними в линейке неисправных плагинов WordPress, появившихся за последние месяцы.

В октябре были обнаружены две высокозащищенные уязвимости в Post Grid, плагине WordPress, у которого установлено более 60 000 экземпляров, которые открывают путь к захвату сайтов. Для начала, почти идентичные ошибки обнаружены и в дочернем плагине Post Grid, Team Showcase, у которого 6000 установок.

В сентябре было обнаружено, что серьезная ошибка в плагине Email Subscribers & Newsletters от Icegram затронула более 100 000 веб-сайтов WordPress.

Ранее, в августе, плагин, предназначенный для добавления викторин и опросов на веб-сайты WordPress, исправил две критические уязвимости. Бреши могут быть использованы удаленными злоумышленниками, не прошедшими

проверку подлинности, для запуска различных атак, в том числе полного захвата уязвимых веб-сайтов. Также в августе Newsletter, плагин WordPress с более чем 300 000 установок, был обнаружен с парой уязвимостей, которые могли привести к выполнению кода и даже захвату сайта.

А в июле исследователи предупредили о критической уязвимости в плагине WordPress под названием Comments - wpDiscuz, который установлен на более чем 70 000 веб-сайтов. Уязвимость давала неаутентифицированным злоумышленникам возможность загружать произвольные файлы (включая файлы PHP) и в конечном итоге выполнять удаленный код на уязвимых серверах веб-сайтов». ***(Tara Seals. Critical WordPress-Plugin Bug Found in 'Orbit Fox' Allows Site Takeover // Threatpost (https://threatpost.com/orbit-fox-wordpress-plugin-bugs/163020/). 13.01.2021).***

***

«Cisco устранила серьезные недостатки, связанные с 67 CVE, в том числе обнаруженные в клиенте AnyConnect Secure Mobility Client и в его маршрутизаторах для малого бизнеса RV110W, RV130, RV130W и RV215W.

Серьезный недостаток интеллектуального решения Cisco Wi-Fi для розничных продавцов может позволить удаленному злоумышленнику изменить пароль любого пользователя учетной записи в уязвимых системах.

Уязвимость является частью ряда исправлений, выпущенных Cisco для 67 серьезных CVE в среду. Это включало недостатки, обнаруженные в клиенте Cisco AnyConnect Secure Mobility Client, а также в маршрутизаторах Cisco RV110W, RV130, RV130W и RV215W для малого бизнеса.

Самый серьезный недостаток связан с Cisco Connected Mobile Experiences (CMX), программным решением, используемым розничными продавцами для предоставления бизнес-аналитики или анализа клиентского опыта на месте. Решение использует беспроводную инфраструктуру Cisco для сбора огромного количества данных из сети Wi-Fi продавца, включая отслеживание местоположения клиентов в реальном времени.

Например, если покупатель подключается к сети Wi-Fi магазина, в котором используется CMX, розничные продавцы могут отслеживать свое местонахождение на месте, наблюдать за их поведением и доставлять им специальные предложения или рекламные акции, пока они там.

Уязвимость (CVE-2021-1144) связана с некорректной обработкой авторизационных проверок для смены пароля. По шкале критичности уязвимости CVSS уязвимость занимает 8,8 балла из 10, что делает ее серьезной. Следует отметить, что для использования уязвимости злоумышленник должен иметь аутентифицированную учетную запись CMX, но ему не потребуются права администратора.

«Злоумышленник, прошедший проверку подлинности без административных привилегий, может воспользоваться этой уязвимостью, отправив измененный HTTP-запрос на уязвимое устройство», - заявила Cisco. «Успешный эксплойт может позволить злоумышленнику изменить пароли любого пользователя в

системе, включая пользователя с правами администратора, а затем выдать себя за этого пользователя».

Администраторы имеют различные привилегии, в том числе возможность использовать команды протокола передачи файлов (FTP) для резервного копирования и восстановления данных на Cisco CMX и получения доступа к учетным данным (для разблокировки пользователей, которым были заблокированы их учетные записи).

Эта уязвимость затрагивает выпуски Cisco CMX 10.6.0, 10.6.1 и 10.6.2; проблема исправлена в выпусках Cisco CMX 10.6.3 и позже.

Другие серьезные недостатки

Другой недостаток высокой степени серьезности (CVE-2021-1237) существует в клиенте Cisco AnyConnect Secure Mobility Client для Windows. AnyConnect Secure Mobility Client, модульный программный продукт для конечных точек, предоставляет широкий спектр услуг безопасности (таких как удаленный доступ, функции веб-безопасности и защита от роуминга) для конечных точек.

Уязвимость позволяет злоумышленникам - если они аутентифицированы и локальны - выполнять атаку путем внедрения библиотеки динамической компоновки (DLL). По словам Cisco, для использования этой уязвимости злоумышленник должен иметь действительные учетные данные в системе Windows.

«Злоумышленник может воспользоваться этой уязвимостью, вставив файл конфигурации по определенному пути в системе, что, в свою очередь, приведет к загрузке вредоносного файла DLL при запуске приложения», - утверждает Cisco. «Успешный эксплойт может позволить злоумышленнику выполнить произвольный код на зараженной машине с системными привилегиями».

Шестьдесят из этих CVE существуют в веб-интерфейсе управления маршрутизаторами Cisco Small Business RV110W, RV130, RV130W и RV215W. Эти недостатки могут позволить прошедшему проверку подлинности удаленному злоумышленнику выполнить произвольный код или вызвать неожиданный перезапуск устройства.

«Злоумышленник может воспользоваться этими уязвимостями, отправив обработанные HTTP-запросы на уязвимое устройство», - утверждает Cisco. «Успешный эксплойт может позволить злоумышленнику выполнить произвольный код от имени пользователя root в базовой операционной системе или вызвать перезагрузку устройства, что приведет к отказу в обслуживании (DoS)».

И еще пять CVE (CVE-2021-1146, CVE-2021-1147, CVE-2021-1148, CVE-2021-1149 и CVE-2021-1150) в маршрутизаторах Cisco Small Business RV110W, RV130, RV130W и RV215W. может позволить аутентифицированному удаленному злоумышленнику вводить произвольные команды, которые выполняются с привилегиями root…». ***(Lindsey O'Donnell. High-Severity Cisco Flaw Found in CMX Software For Retailers // Threatpost (https://threatpost.com/cisco-flaw-cmx-software-retailers/163027/). 13.01.2021).***

***

«Исследователь безопасности из австрийской компании SEC Consult обнаружил ряд уязвимостей в промышленных шлюзах Pepperl+Fuchs Comtrol IO-Link Master. Эксплуатация уязвимостей позволяет получить корневой доступ к устройству и создавать бэкдоры.

Обнаруженные проблемы представляют собой уязвимости подделки межсайтовых запросов (CVE-2020-12511), межсайтового скриптинга (CVE-2020-12512), слепого внедрения команд (CVE-2020-12513) и вызова состояния «отказа в обслуживании» (CVE-2020-12514). Уязвимые продукты используют устаревшие версии сторонних компонентов, включая PHP, OpenSSL, BusyBox, ядро Linux и lighttpd, которые, как известно, содержат различные проблемы.

По словам эксперта, если злоумышленник получит доступ к одному из уязвимых устройств Comtrol, он сможет выполнить команды на устройстве с привилегиями суперпользователя и внедрить постоянные бэкдоры.

Поставщик исправил уязвимости, обнаруженные SEC Consult, через несколько месяцев после того, как получил уведомление. SEC Consult также опубликовала уведомление безопасности, содержащее PoC-код для эксплуатации каждой из уязвимостей». ***(Уязвимости в продуктах Pepperl+Fuchs позволяют внедрять бэкдоры // SecurityLab.ru (https://www.securitylab.ru/news/515538.php). 15.01.2021).***

***

«Исследователи из компании Check Point, занимающейся кибербезопасностью, заявили во вторник, что уязвимость, обнаруженная в популярном приложении для обмена видео TikTok, подвергает пользователей извлечению личной информации из их профиля, включая номер телефона и настройки профиля. По словам исследователей, эта информация могла быть использована для манипулирования данными учетных записей пользователей и создания базы данных пользователей TikTok на предмет злонамеренных действий.

По словам Check Point, из-за недостатка в функции «Найти друзей» были обнаружены никнеймы пользователей, изображения профилей и аватаров, а также уникальные идентификаторы пользователей. Нет никаких доказательств того, что уязвимость когда-либо использовалась, и, как сообщается, недостаток был исправлен.

«Злоумышленник с такой степенью конфиденциальной информации может выполнить ряд злонамеренных действий, таких как целевой фишинг или другие преступные действия», - говорится в заявлении официального представителя Check Point Экрама Ахмеда. «Мы обращаемся к пользователям TikTok с просьбой поделиться минимумом, когда дело касается ваших личных данных».

TikTok назвал безопасность и конфиденциальность в своем сообществе своим наивысшим приоритетом и поблагодарил Check Point за то, что они обратили внимание на уязвимость.

«Мы продолжаем укреплять нашу защиту, постоянно совершенствуя наши внутренние возможности, такие как инвестирование в средства защиты автоматизации, а также работая с третьими сторонами», - говорится в заявлении представителя TikTok.

TikTok, который работает за пределами Китая, но принадлежит китайской технологической компании ByteDance, столкнулся со своей долей разногласий, когда дело доходит до безопасности пользовательских данных. В 2019 году пользователь из Калифорнии подал на компанию в суд, утверждая, что TikTok делится пользовательскими данными с правительством Китая. Армия США запретила военнослужащим использовать приложение на правительственных телефонах после первоначального использования службы для вербовки.

Это также не первая уязвимость TikTok, обнаруженная TikTok. Ранее в этом месяце исследователи компании выявили в приложении серию программных недостатков, которые открыли дверь для ряда атак на пользователей, включая отправку текстовых сообщений со ссылками на вредоносное ПО и манипулирование видео, хранящимися в сервисе». ***(Steven Musil. TikTok vulnerability left users' private information exposed // CNET (https://www.cnet.com/news/tiktok-vulnerability-left-users-private-information-exposed/). 26.01.2021).***

***

«ProtonVPN работает над исправлением ошибки, приводящей к сбою "синего экрана" Windows, затрагивающей клиентов, использующих последние версии клиентского программного обеспечения Windows компании.

Сбои BSOD не затрагивают всех пользователей и вызваны конфликтами с неназванными антивирусными программными решениями.

«Мы получили сообщения о том, что при определенных обстоятельствах последние версии клиентов ProtonVPN для Windows (стабильная версия 1.18.2 и версия с ранним доступом 1.18.3) могут приводить к сбою синего экрана в Windows из-за конфликта с определенными антивирусами, "ProtonVPN сказал.

«Мы активно работаем над исправлением, которое будет доступно в ближайшее время», - добавила компания в заявлении о статусе инцидента, открытом на выходных.

Затронутым клиентам рекомендуется отключить антивирус, чтобы предотвратить сбои системы, или понизить версию своего клиента ProtonVPN.

«Если вас затронула такая ситуация, мы советуем либо временно отключить антивирус, который может вступить в конфликт при использовании ProtonVPN, либо перейти на предыдущую стабильную версию», - заявили в компании.

Синие экраны срабатывают сразу после запуска

Хотя ProtonVPN не раскрыл более подробную информацию о причинах стоп-ошибок, более подробная информация была предоставлена в пользовательских отчетах о синих экранах Windows, вызванных последней версией ProtonVPN, появившейся около двух недель назад.

В качестве одного из пострадавших пользователей совместно, синие экраны срабатывают сразу же после запуска клиента виртуальной частной сети в Windows.

Это не первый раз, когда пользователи сообщают о сбоях синего экрана на своих компьютерах с Windows при использовании ProtonVPN.

В то время клиенты в комментариях [1, 2] добавили к статье поддержки ProtonVPN о проблемах с подключением к Windows, что их системы будут давать сбой после аутентификации или после установления VPN-туннеля.

Как и в случае с текущей ошибкой, затрагивающей стабильные клиенты ProtonVPN с ранним доступом для Windows, переустановка клиента и драйверов не поможет». ***(Sergiu Gatlan. ProtonVPN causes Windows BSOD crashes due to antivirus conflicts // Bleeping Computer (https://www.bleepingcomputer.com/news/software/protonvpn-causes-windows-bsod-crashes-due-to-antivirus-conflicts/). 25.01.2021).***

***

«В этом месяце инженеры Google устранили серьезную уязвимость удаленного выполнения кода (RCE) в языке Go (Golang).

Уязвимость RCE, CVE-2021-3115, в основном затрагивает пользователей Windows Go, выполняющих go get команду, из-за поведения по умолчанию при поиске PATH в Windows.

RCE из поиска PATH в ненадежных каталогах

Недавно японский исследователь безопасности RyotaK обнаружил уязвимость внедрения команд в проекте Golang.

Уязвимость, обозначенная как CVE-2021-3115, связана с тем, как работает процесс компиляции, когда пользователь запускает команду «go get» для получения репозитория.

Как правило, в системах Windows команда оболочки ОС, запускаемая пользователем или программой, заставляет оболочку сначала искать двоичный / исполняемый файл, связанный с этой командой, в текущем каталоге, а затем список каталогов, указанный в системной переменной PATH.

Например, если вы netstat введете командную строку Windows, Windows сначала будет искать в текущем каталоге исполняемый файл netstat.exe, netstat.bat или другой исполняемый файл netstat. * (См. Снимок экрана ниже), который получит приоритет и будет выполнен.

Если в текущей папке нет netstat, только тогда оболочка Windows будет искать системную утилиту netstat, расположение которой указано в переменной Windows % PATH%.

Из-за рисков безопасности, связанных с таким поведением, и оболочка Unix, и Windows PowerShell ранее отказались от этого поведения по умолчанию и начали отдавать приоритет расположениям переменных% PATH% над ненадежным текущим каталогом при выполнении команд.

Это означает, что запуск netstat в PowerShell запустит системную утилиту netstat, а не локально присутствующий netstat.bat, поскольку PoweShell отдает приоритет поиску двоичного файла по этому имени в каталогах% PATH%.

Однако для согласованности двоичные файлы Golang имитируют правила Unix в системах Unix и правила Windows в Windows.

Это означает, что выполнение следующей команды Go приведет к несколько разному поведению в системах Unix и Windows.

Эта строка Golang эквивалентна запуску команды go version оболочки ОС.

В Windows локально присутствующий двоичный файл go получит приоритет, тогда как системы Unix сначала будут искать свою переменную $ PATH, чтобы увидеть, существует ли двоичный файл go в одном из надежных расположений.

Эта модель приоритета локального, ненадежного каталога над местоположениями PATH также реализуется вспомогательными библиотеками и компиляторами, включенными в Go, такими как cgo, утилита, предназначенная для генерации пакетов Go, которые вызывают код C.

Когда cgo компилирует код C в Windows, в конечном итоге исполняемый файл Golang сначала ищет компилятор GCC в (ненадежном) локальном каталоге.

«Когда go get загружает и создает пакет, содержащий import «C», он запускает программу cgo для подготовки Go-эквивалента соответствующего кода C.»

«Команда go запускает cgo в каталоге, содержащем исходные коды пакетов, - объясняет инженер Google Расс Кокс.

Хотя большинство этих вызовов происходит безопасным образом, компилятор GCC вызывается функцией Go exec.Command, которая в Windows позволяет Go запускать вредоносный gcc.exe, включенный злоумышленником в свои источники приложений, а не законный компилятор GCC.

Может показаться, что эту неудачу можно было поймать и предотвратить с помощью нескольких вызываемых промежуточных компиляторов и библиотек (например, cgo или gcc), но проект Golang взял на себя ответственность за ошибку и выпустил исправление.

«Однако сегодняшняя ошибка была полностью нашей ошибкой, а не ошибкой или неясной особенностью gcc или git».

«Ошибка связана с тем, как Go и другие программы находят другие исполняемые файлы, поэтому нам нужно потратить немного времени на изучение этого, прежде чем мы сможем перейти к деталям», - говорит Кокс.

Исследователь, вдохновленный более ранней критической уязвимостью

BleepingComputer обратился к RyotaK, чтобы узнать больше о том, как он обнаружил эту уязвимость.

Оказывается, чтение о критической уязвимости внедрения команд в Git LFS, CVE-2020-27955, и вдохновило исследователя на поиски аналогичной уязвимости в самом Golang.

«Я обнаружил эту уязвимость из-за CVE-2020-27955. Это было удаленное выполнение кода в Git LFS, вызванное небезопасным выполнением файла».

«Проверяя технические детали [ошибки], я подумал: «Может ли эта уязвимость быть затронута в официальном проекте Go?»

«А затем я начал читать репозитории, принадлежащие организации golang. Вскоре после этого я обнаружил эту уязвимость вместе с некоторыми другими уязвимостями, имеющими ту же основную причину».

«Поскольку эта уязвимость может позволить выполнение произвольного кода при построении вредоносного кода на Windows, это может повлиять на системы, которые ожидают Go не может выполнить произвольный код во время сборки,» RyotaK сказал BleepingComputer в интервью по электронной почте.

Однако, чтобы удаленный злоумышленник мог воспользоваться этой уязвимостью, пользователю необходимо запустить команду go get против вредоносного репозитория.

«Это требует некоторого взаимодействия со стороны жертвы; им нужно запустить «иди иди» против вредоносного репозитория», - сказал исследователь BleepingComputer.

Команда Golang в Google устранила уязвимость, и пользователям рекомендуется обновить свои экземпляры.

Пользователи могут обновиться до недавно выпущенных версий Go 1.14.14 (для 1.14.x и более ранних) и 1.15.7 (для пользователей 1.15.x), чтобы уменьшить эту уязвимость.

Кроме того, разработчики Google также выпустили исправление для криптографической уязвимости CVE-2021-3114, о которой сообщил Филипп Антуан из Catena Cyber в тех же выпусках.

Ожидается, что предстоящий выпуск Go 1.16rc1 также будет включать исправления для CVE-2021-3114 и CVE-2021-3115». ***(Ax Sharma. Google fixes severe Golang Windows RCE vulnerability // Bleeping Computer (https://www.bleepingcomputer.com/news/security/google-fixes-severe-golang-windows-rce-vulnerability/). 26.01.2021).***

***

«Исправленная уязвимость Sudo позволила любому локальному пользователю получить привилегии root в Unix-подобных операционных системах без необходимости аутентификации.

Sudo - это программа для Unix, которая позволяет системным администраторам предоставлять ограниченные привилегии root обычным пользователям, перечисленным в файле sudoers, и в то же время вести журнал их активности.

Он работает по принципу наименьших привилегий, согласно которому программа дает людям достаточно разрешений, чтобы выполнять свою работу без ущерба для общей безопасности системы.

При выполнении команд в Unix-подобной ОС непривилегированные пользователи могут использовать команду sudo (superuser do) для выполнения команд от имени пользователя root, если они имеют разрешение или знают пароль пользователя root - root - это суперпользователь системы, специальная учетная запись системного администратора.

Sudo также можно настроить так, чтобы обычные пользователи могли запускать команды как любой другой пользователь, включив специальные директивы в файл конфигурации sudoers.

Права root для любого локального пользователя

Уязвимость повышения привилегий Sudo, отслеживаемая как CVE-2021-3156 (также известная как Baron Samedit), была обнаружена исследователями безопасности из Qualys, которые раскрыли ее 13 января и удостоверились, что исправления доступны, прежде чем обнародовать свои результаты.

По мнению исследователей Qualys, проблема заключается в переполнении буфера на основе кучи, которое может использовать любой локальный пользователь (обычные пользователи и системные пользователи, указанные в файле sudoers или нет), при этом злоумышленникам не требуется знать пароль пользователя для успешного использования уязвимости.

Переполнение буфера, позволяющее любому локальному пользователю получить привилегии root, запускается Sudo, неправильно удаляющим обратную косую черту в аргументах.

«Обычно sudo экранирует специальные символы при запуске команды через оболочку (sudo -s или sudo -i)», - говорится в журнале изменений 1.9.5p2.

«Однако можно было запустить sudoedit с флагами -s или -i, и в этом случае экранирование не было выполнено, что сделало возможным переполнение буфера».

Qualys создала три эксплойта CVE-2021-3156, чтобы продемонстрировать, как потенциальные злоумышленники могут успешно использовать эту уязвимость.

Используя эти эксплойты, исследователи смогли получить полные привилегии root в нескольких дистрибутивах Linux, включая Debian 10 (Sudo 1.8.27), Ubuntu 20.04 (Sudo 1.8.31) и Fedora 33 (Sudo 1.9.2).

Другие операционные системы и дистрибутивы, поддерживаемые Sudo, вероятно, также могут использоваться с использованием эксплойтов CVE-2021-3156, согласно Qualys.

Дополнительные технические подробности о том, как можно использовать CVE-2021-3156, доступны в рекомендациях Qualys по безопасности CVE-2021-3156, опубликованных во вторник…

Недостаток Барона Самедита исправлен до раскрытия

Уязвимость была представлена в программе Sudo почти 9 лет назад, в июле 2011 года, с фиксацией 8255ed69, и она затрагивает конфигурации по умолчанию всех стабильных версий от 1.9.0 до 1.9.5p1 и всех устаревших версий от 1.8.2 до 1.8.31p2.

Авторы Sudo устранили уязвимость в версии sudo 1.9.5p2, выпущенной ранее сегодня, в то же время Qualys публично раскрыла свои выводы.

Чтобы проверить, уязвима ли ваша система, вы должны войти в систему как пользователь без полномочий root и выполнить команду «sudoedit -s /». Уязвимые системы будут выдавать ошибку, начинающуюся с «sudoedit:», в то время как исправленные системы отображают ошибку, начинающуюся с «usage:».

Системные администраторы, которые используют Sudo для делегирования полномочий root своим пользователям, должны как можно скорее перейти на sudo 1.9.5p2 или более позднюю версию.

В 2019 году еще одна уязвимость Sudo, отслеживаемая как CVE-2019-14287, позволила непривилегированным пользователям выполнять команды от имени пользователя root.

К счастью, этот недостаток можно было использовать только в нестандартных конфигурациях, а это означало, что большинство систем с уязвимыми версиями Sudo не пострадали». ***(Sergiu Gatlan. New Linux SUDO flaw lets local users gain root privileges // Bleeping Computer***

(https://www.bleepingcomputer.com/news/security/new-linux-sudo-flaw-lets-local-users-gain-root-privileges/). 26.01.2021).

***

«Drupal выпустила обновление безопасности для устранения критической уязвимости в сторонней библиотеке с документированными или развернутыми эксплойтами, доступными в дикой природе.

«Проект Drupal использует библиотеку pear Archive_Tar, которая выпустила обновление безопасности, которое влияет на Drupal», - заявила группа безопасности Drupal.

Drupal используется примерно 2,4% всех сайтов с системами управления контентом, что делает его пятым по популярности CMS в Интернете после WordPress (64,1%), Shopify (5,2%), Joomla (3,5%) и Squarespace (2,5%).

Обновления безопасности для всех уязвимых версий

Согласно рекомендациям по безопасности Drupal, уязвимость вызвана ошибкой в библиотеке PEAR Archive_Tar, используемой CMS, которая отслеживается как CVE-2020-36193.

Ошибка вызывает уязвимости извлечения вне пути через «операции записи с обходом каталогов из-за неадекватной проверки символических ссылок».

Для успешной эксплуатации требуется доступ к учетным записям пользователей с базовыми разрешениями на серверах с необычными конфигурациями модулей.

Использование уязвимости Drupal возможно только в том случае, если CMS настроена на разрешение и обработку загрузки файлов .tar, .tar.gz, .bz2 или .tlz.

После эксплуатации злоумышленники могут изменить или удалить все данные, а также получить доступ ко всем закрытым данным, доступным на скомпрометированном сервере.

Drupal рекомендует установить следующие обновления на уязвимых серверах:

Пользователи Drupal 9.1 должны обновиться до Drupal 9.1.3

Пользователи Drupal 9.0 должны обновиться до Drupal 9.0.11

Пользователи Drupal 8.9 должны обновиться до Drupal 8.9.13

Пользователи Drupal 7 должны обновиться до Drupal 7.78

«Версии Drupal 8 до 8.9.x являются устаревшими и не получают защиты», - добавили специалисты службы безопасности Drupal.

Эта уязвимость связана с другим критическим недостатком безопасности с известными эксплойтами, вызванным ошибкой CVE-2020-28948 в библиотеке PEAR Archive_Tar, которая может допускать выполнение произвольного кода PHP в некоторых версиях CMS.

В ноябре Drupal выпустил внешнее экстренное обновление безопасности, чтобы исправить это, что позволяет администраторам быстро исправлять свои серверы, чтобы защитить их от потенциальных атак.

Доступны меры по смягчению последствий

Меры по смягчению доступны для администраторов, которые не могут немедленно развернуть обновление безопасности на своих серверах Drupal.

Для этого им рекомендуется отключить загрузку файлов .tar, .tar.gz, .bz2 или .tlz, чтобы временно уменьшить проблему.

DHS-CISA также выпустило в четверг предупреждение, призывающее администраторов и пользователей обновить Drupal, чтобы не дать злоумышленникам захватить непропатченные серверы.

Drupal исправил еще одну критическую уязвимость удаленного выполнения кода, отслеживаемую как CVE-2020-13671 и позволяющую злоумышленникам выполнять вредоносный код на уязвимых серверах из-за неправильной очистки имен файлов для загруженных файлов.

«Обратите особое внимание на следующие расширения файлов, которые следует считать опасными, даже если за ними следует одно или несколько дополнительных расширений: phar, PHP, pl, py, cgi, asp, js, HTML, htm и phtml», - сказал Друпал на время.

«Этот список не является исчерпывающим, поэтому оценивайте проблемы безопасности для других неотключенных расширений в индивидуальном порядке». ***(Sergiu Gatlan. Drupal releases fix for critical vulnerability with known exploits // Bleeping Computer (https://www.bleepingcomputer.com/news/security/drupal-releases-fix-for-critical-vulnerability-with-known-exploits/). 22.01.2021).***

***

«В случае эксплуатации наиболее серьезные из этих недостатков могут привести к отказу в обслуживании продуктов Jetson.

Nvidia устранила три уязвимости, влияющие на линейку Jetson, которая представляет собой серию встраиваемых вычислительных плат, предназначенных для приложений машинного обучения, таких как автономные роботы, дроны и многое другое. По словам Nvidia, успешный эксплойт потенциально может вывести из строя любые такие устройства, использующие затронутые продукты Jetson.

В случае использования наиболее серьезные из этих недостатков могут привести к отказу в обслуживании (DoS) для затронутых продуктов. Дефект (CVE-2021-1070) занимает 7,1 балла из 10 по шкале CVSS, что делает его серьезным. Он специально существует в пакете драйверов Nvidia Linux (L4T), пакете поддержки плат для продуктов Jetson.

Nvidia L4T содержит сбой в скрипте apply_binaries.sh. Этот сценарий используется для установки компонентов Nvidia в образ корневой файловой системы. Сценарий допускает неправильный контроль доступа, что может привести к тому, что непривилегированный пользователь сможет изменять файлы дерева системных устройств. Деревья устройств - это структура данных аппаратных компонентов конкретного компьютера, которая позволяет ядру операционной системы использовать и управлять этими компонентами, включая ЦП, память и периферийные устройства.

Доступ к файлу дерева устройств может позволить злоумышленнику запустить DoS-атаку. Более подробная информация об уязвимости, в том числе о том, что нужно злоумышленнику для ее использования, не разглашается. Проблема была обнаружена программистом Майклом де Гансом.

Все версии до L4T выпуска r32.5 затронуты; патч доступен в версии L4T r32.5. Конкретные затронутые продукты Jetson включают серии Jetson TX1 и TX2; которые представляют собой две маломощные встраиваемые вычислительные платы с процессором Nvidia Tegra, специально разработанные для ускорения машинного обучения в системах. Также затронуты серия Jetson AGX Xavier, комплект разработчика, который по сути представляет собой компьютер с искусственным интеллектом для автономных машин; комплект разработчика Jetson Xavier NX; и комплекты разработчика Jetson Nano и Jetson Nano 2 ГБ.

Два других - это недостатки средней степени серьезности (CVE - 2021-1069 и CVE - 2021-1071), которые были обнаружены в драйвере ядра Nvidia Tegra. Это код, который позволяет ядру взаимодействовать с аппаратными устройствами, в которых находится система на кристалле (SoC).

CVE - 2021-1069 существует в NVHost, программном хосте, который является частью службы поддержки драйверов Nvidia. NVHost позволяет переменной иметь значение NULL, что может привести к разыменованию нулевого указателя и неожиданной перезагрузке, что в конечном итоге приведет к потере данных, согласно Nvidia.

Между тем CVE - 2021-1071 существует в драйвере INA3221, встроенном мониторе мощности, который контролирует напряжение и ток определенных шин. Недостаток делает возможным неправильный контроль доступа, что может привести к тому, что неавторизованные пользователи получат доступ к данным об использовании энергии системой. Это может привести к раскрытию информации.

Это только последний набор патчей, который Nvidia выпустит в этом месяце. На прошлой неделе Nvidia недавно обнаружила три уязвимости в системе безопасности NVIDIA Shield TV, которые могут привести к отказу в обслуживании, повышению привилегий и потере данных. Ранее в январе Nvidia исправила недостатки, связанные с 16 CVE в своих графических драйверах и программном обеспечении vGPU, в своем первом обновлении безопасности в 2021 году. Обновленные рекомендации по безопасности теперь включают наличие исправленных драйверов Linux для линейки графических процессоров Tesla, влияющих на CVE-2021. -1052, CVE-2021-1053 и CVE-2021-1056». ***(Lindsey O'Donnell. Nvidia Squashes High-Severity Jetson DoS Flaw // Threatpost (https://threatpost.com/nvidia-squashes-high-severity-jetson-dos-flaw/163360/). 26.01.2021).***

***

«Некогда участник известного хактивистского движения LulzSec, а теперь исследователь безопасности Даррен Мартин (Darren Martyn) опубликовал эксплоит для уязвимости в VPN-приложении SonicWall. Эксплоит предназначен для уязвимостей, эксплуатировавшихся хакером Phineas Fisher для взлома итальянского производителя хакерских инструментов Hacking Team.

Мартин опубликовал эксплоит в своем блоге в понедельник, 25 января – через день после того, как компания SonicWall сообщила о проникновении злоумышленников в ее сети через уязвимость нулевого дня в ее же оборудовании.

По словам исследователя, он решил опубликовать эксплоит, чтобы продемонстрировать проблемы с безопасностью у SonicWall.

«Учитывая новости о том, что SonicWall была взломана через уязвимости нулевого дня в ее же собственных продуктах, было бы забавно опубликовать это», - сообщил Мартин.

Исследователь написал эксплоит после ознакомления с описанием атаки на офшорный банк в 2019 году, представленным хакером Phineas Fisher. По словам Phineas Fisher, в ходе взлома финорганизации он проэксплуатировал уязвимость нулевого дня в используемом банком VPN-решении SonicWall. Эта же уязвимость использовалась хакером в атаке на Hacking Team в 2015 году.

После прочтения публикации Phineas Fisher Мартин смог создать собственный эксплоит всего за две минуты. По словам исследователя, в описании атаки есть «все что нужно» для этого.

Как сообщает SonicWall, эксплуатировавшиеся в атаках уязвимости были исправлены в 2015 году с выходом SonicWall SMA 8.0.0.4, и проэксплуатировать их в версиях SonicWall SMA 9 и 10 нельзя.

Последний шаг в цепочке эксплуатации уязвимости – получение административных привилегий в SonicWall VPN, исследователь решил не публиковать, чтобы малоопытные хакеры не смогли просто скопировать эксплоит и использовать его во вред». ***(Экс-участник LulzSec опубликовал эксплоит для уязвимости в SonicWall VPN // SecurityLab.ru (https://www.securitylab.ru/news/515951.php). 26.01.2021).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Фирма по кибербезопасности Bitdefender сегодня выпустила бесплатный инструмент, который может помочь жертвам вымогателя Darkside бесплатно восстановить свои зашифрованные файлы, не платя требования выкупа.

Инструмент, доступный для загрузки с сайта Bitdefender вместе с инструкциями по использованию, дает надежду компаниям, у которых важные файлы были заблокированы и выкуплены в результате одной из самых сложных операций вымогателей на сегодняшний день.

ПРЕДЫСТОРИЯ ГРУППЫ DARKSIDE

Группа Darkside, действующая с лета 2020 года, начала свою деятельность и до сих пор действует через рекламу, размещенную на форумах по киберпреступности.

Группа использует хорошо зарекомендовавшую себя модель «Программа-вымогатель как услуга» (RaaS) для сотрудничества с другими группами киберпреступников.

Эти группы подадут заявку на Darkside RaaS и получат полнофункциональную версию программы-вымогателя Darkside. Затем они взламывали компании, используя выбранные ими методы, устанавливали программы-вымогатели и запрашивали огромные выплаты, обычно в размере сотен тысяч или миллионов долларов США.

Этот способ работы не нов, и он называется «охотой на крупную дичь», потому что банды вымогателей обычно охотятся за компаниями, а не за домашними пользователями, в надежде увеличить свою прибыль.

В ситуациях, когда жертвы не хотят платить, операторы Darkside сливают документы, которые они украли из сети жертвы, на специальном «сайте утечки» в качестве наказания и предупреждения другим жертвам, которые могут захотеть восстановить данные из резервных копий вместо того, чтобы платить мошенники.

Хотя Darkside не публиковал имена и данные каких-либо новых жертв на своем сайте утечки с момента перед зимними праздниками в прошлом году, группа все еще считается активной на момент написания.

По словам исследователя безопасности MalwareHunter, последняя активность группы - это обновление ее сайта утечки на прошлой неделе, во время которого операторы Darkside добавили новый раздел, посвященный журналистам, где репортеры могут зарегистрироваться и напрямую связаться с бандой Darkside.

В то время как большинство жертв Darkside либо уже заплатили требование выкупа, либо восстановлены из резервной копии несколько месяцев назад, дешифратор Darkside не совсем бесполезен, но это далеко не так.

ПРИВЕДЕТ ЛИ ДЕШИФРАТОР К ОТКЛЮЧЕНИЮ DARKSIDE?

Прежде всего, этот инструмент помогает компаниям восстанавливать важные файлы, которые были зашифрованы несколько месяцев назад и которые они не смогли восстановить, но все еще хранятся на резервных дисках.

Во-вторых, инструмент также несет операционные расходы банде Darkside, которая теперь должна будет заново выполнить весь свой код шифрования файлов, чтобы предотвратить бесплатное дешифрование.

В-третьих, инструмент также наносит серьезный удар по репутации Darkside RaaS. Многие операции с программами-вымогателями были прекращены в прошлом после выпуска бесплатного дешифратора, поскольку большинство их клиентов отказались от них в пользу более новых и не поддающихся дешифрованию конкурентов.

Что касается самих жертв, то хорошей новостью является то, что бесплатный дешифратор, выпущенный сегодня Bitdefender, теоретически должен работать со всеми последними версиями вымогателя Darkside, независимо от расширения файла, которое мошенники добавили в конец каждого зашифрованного файла.

По словам Bitdefender, это расширение является уникальным для каждой жертвы, поскольку оно рассчитывается на основе локальных характеристик, но это не должно быть проблемой». ***(Catalin Cimpanu. Free decrypter released for victims of Darkside ransomware // ZDNet (https://www.zdnet.com/article/free-decrypter-released-for-victims-of-darkside-ransomware/). 11.01.2021).***

***

«Varonis расширила функциональность своего флагманского решения — платформы кибербезопасности Varonis.

Переход на удаленный режим работы привел к росту популярности инструментов для совместной работы сотрудников. Например, число активных пользователей Microsoft Teams выросло с 75 млн в день (на апрель 2020 г.) до 115 млн в день (на октябрь 2020), и эта цифра продолжает расти. В условиях большого объема данных, создаваемых и передаваемых через приложения для совместной работы, офицерам по информационной безопасности все сложнее отслеживать, где хранятся, кем и куда передаются конфиденциальные данные. Использование встроенных средств безопасности Microsoft не решает этой проблемы, отмечают в Varonis.

С помощью новых возможностей платформы кибербезопасности Varonis стало возможным закрыть «слепые зоны», связанные с уязвимостью конфиденциальных данных, появляющихся в облаке при совместной работе в Microsoft 365 и других облачных приложениях.

Платформа кибербезопасности Varonis позволяет автоматизировать процессы защиты критически важной информации, обеспечивать соответствие принципам «нулевого доверия», решать задачи по обеспечению конфиденциальности и соблюдения нормативных требований, а также обнаруживать современные киберугрозы, исходящие как извне, так и от инсайдеров.

Среди новых опций: анализ всего спектра угроз в Microsoft 365. Новые дашборды на панели мониторинга показывают, когда ссылки для совместной работы, общедоступные сайты и избыточные права доступа открывают информацию слишком большому количеству сотрудников; расширенное обнаружение угроз и обновление индикаторов компрометации (IOC). Дополнительные модели угроз для Azure AD помогают предотвратить атаки на клиентские среды Microsoft 365, а автоматические обновления IOC помогают защититься от новых угроз, таких как уязвимость Zerologon и Sunburst; больше возможностей для детального поиска чувствительных данных. Новые поисковые возможности позволяют раскрывать логику запросов и эффективнее находить конфиденциальные данные в локальных и облачных хранилищах данных; расширение поддержки сетевых хранилищ. Поддержка Panzura, EMC NAS, Nasuni 8.5, Hitachi NAS и NetApp Ontap Select 9.7, а также пространств имен кластера Hitachi NAS.

«Microsoft 365 упрощает обмен конфиденциальными данными с вашими коллегами и гостевыми пользователями, но эффективно обнаруживать и контролировать риски совместной работы с помощью встроенных инструментов практически невозможно. Новые возможности версии 8.5 платформы кибербезопасности Varonis предоставят ИТ-специалистам и специалистам по безопасности четкое представление о том, как пользователи обмениваются информацией для быстрого отслеживания и устранения рисков уязвимости данных и от внутренних угроз и кибератак», — сказал Дэвид Гибсон, директор по маркетингу компании Varonis». ***(Varonis расширила функциональность своей платформы кибербезопасности // CNews (https://safe.cnews.ru/news/line/2021-01-25_varonis_rasshirila_funktsionalnost). 25.01.2021).***

***

«Windows 10X - это новая оптимизированная версия Windows, разработанная для обеспечения безопасности и производительности, которую Microsoft объявила в 2019 году и планирует выпустить весной 2021 года на новом диапазоне устройств.

До сих пор многие детали были скудными, но благодаря сборке Windows 10X, которая просочилась на прошлой неделе, мы можем хорошо изучить операционную систему и ее функции.

В дополнение к новому пользовательскому интерфейсу Windows 10X также поставляется с новой функцией, которая называется «Защита от кражи», - мера, предназначенная для предотвращения того, чтобы воры не могли стереть и повторно использовать украденные устройства.

Если устройство с Windows 10 разблокировано, любой может войти в настройки и использовать функцию под названием «Сбросить этот компьютер», чтобы вернуть устройства к заводским настройкам.

Когда в Windows 10X предусмотрена функция защиты от кражи, пользователь должен будет войти в систему с учетной записью Microsoft, ранее связанной с устройством, или ввести PIN-код, прежде чем устройство можно будет сбросить и использовать как новое.

«Защита от кражи не позволяет кому-либо перезагрузить ваше устройство и повторно использовать его. Когда защита от кражи включена, вам нужно будет ввести свой PIN-код или пароль учетной записи Microsoft перед сбросом и повторным использованием этого устройства», - описывает Microsoft в приложении "Настройки".

В Windows 10X вы можете настроить функцию защиты от кражи в разделе «Настройки» > «Защита от кражи».

Поскольку Windows 10X была разработана для портативных устройств, включение функции, затрудняющей сброс нового устройства, делает украденные устройства менее ценной целью. Microsoft использовала аналогичную функцию в Windows Mobile для защиты устройств в случае кражи.

Для Microsoft также имеет смысл перенести эту функцию на обычную операционную систему Windows 10, чтобы обеспечить дополнительную безопасность разблокированным устройствам.

Нет никаких указаний на то, что Microsoft планирует сделать это в настоящее время». ***(Mayank Parmar. Windows 10X feature will prevent unauthorized factory resets // Bleeping Computer (https://www.bleepingcomputer.com/news/microsoft/windows-10x-feature-will-prevent-unauthorized-factory-resets/). 24.01.2021).***

***

«В понедельник компания Google сообщила, что её платформа BeyondCorp Enterprise теперь доступна всем предприятиям, которые хотят воспользоваться преимуществами модели безопасности с нулевым доверием.

BeyondCorp Enterprise является расширением и заменой предложения BeyondCorp Remote Access, которое было запущено в прошлом году для защиты компаний, вынужденных переключиться на удаленную работу из-за пандемии COVID-19. BeyondCorp Remote Access обеспечивала доступ с нулевым доверием только для наиболее ответственных приложений и данных, чтобы сотрудники могли безопасно выполнять свою работу из дома.

В модели с нулевым доверием пользователи, запрашивающие доступ изнутри сети, считаются столь же ненадежными, как и те, кто находится за её пределами. Управление доступом переносится с периметра на отдельные устройства и пользователей, что позволяет сотрудникам безопасно работать из любого места без традиционной виртуальной частной сети.

Новое предложение BeyondCorp Enterprise тесно связано с браузером Chrome, который обеспечивает встроенную защиту от угроз и данных для предотвращения злонамеренной и случайной утечки данных.

С помощью BeyondCorp Enterprise организации могут внедрять дополнительные средства управления аутентификацией, такие как принудительное использование защищенных от фишинга ключей безопасности и непрерывная авторизация, которая учитывает сведения о пользователе, устройстве и геопозиции. На эту платформу также распространяется поддержка высокомасштабируемой службы Google, защищающей от DDoS-атак с трафиком до 2,5 терабайт в секунду.

BeyondCorp Enterprise функционирует незаметно для большинства пользователей. «Лучшая безопасность — это невидимая безопасность», — отметил в блоге вице-президент и генеральный менеджер Google Cloud Security Сунил Потти (Sunil Potti).

Google активно работает над построением экосистемы безопасности с нулевым доверием: альянс BeyondCorp Alliance объединяет поставщиков услуг безопасности и управления данными, включая занимающийся защитой конечных точек стартап Tanium, фирмы Check Point Software Technologies, Lookout, VMware, Palo Alto Networks и корпорацию Symantec». ***(Google объявила о доступности платформы безопасности с нулевым доверием // Компьютерное Обозрение (https://ko.com.ua/google_obyavila_o_dostupnosti_platformy_bezopasnosti_s_nulevym_doveriem_136101). 28.01.2021).***

***

«Компания Elcore Ukraine сообщает о доступности клиентам новейшего демо-оборудования Trend Micro. Как утверждается, на данный момент, этот дистрибьютор единственный не только в Украине, но и на всём пространстве бывшего СНГ может предложить решения линейки TxOne для пилотных проектов.

В линейку TxOne входит EdgeFire – межсетевой экран нового поколения. Он обнаруживает и перехватывает киберугрозы, устанавливая защиту границ и сегментацию между сетями OT и подключенными производственными активами, эффективно предотвращая распространение угроз. EdgeFire также обеспечивает высокий уровень видимости активов и защищает устройства, на которых не установлены исправления, а также указывает на уязвимые устаревшие системы, чтобы минимизировать время простоя для установки исправлений или

дополнительного обслуживания. Благодаря управлению критически важным оборудованием и реагированию на инциденты это решение помогает защитить производственную линию и обеспечить ее бесперебойную работу.

Также линейка защитных решений Trend Micro включает EdgeIPS – систему предотвращения вторжений «следующего поколения» (IPS), которая помогает промышленным средам решать растущие проблемы безопасности, обеспечивая видимость в OT, позволяет устанавливать фильтры для протоколов OT и добавляет другие функции в инструментарий обеспечения киберзащиты. Он защищает ключевые ресурсы, такие как программируемые логические контроллеры (ПЛК) и человеко-машинные интерфейсы (HMI), на сетевом уровне от кибератак, в том числе тех, которые используют червей и уязвимости, тем самым обеспечивая бесперебойную работу производственной линии». ***(Elcore Ukraine предлагает оборудование Trend Micro для пилотных проектов // Компьютерное Обозрение (https://ko.com.ua/elcore_ukraine_predlagaet_oborudovanie_trend_micro_dlya_pilotnyh_proektov_136025). 21.01.2021).***

***