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

# КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

## № 6 (червень)

**Київ – 2021**

**Кібербезпека в інформаційному суспільстві:** Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»; Національна бібліотека України ім. В.І.Вернадського. – К., 2021.– №6 (червень) . – 261 с.

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

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

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

© Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України», 2021
© Національна бібліотека України імені В.І. Вернадського, 2021

# ЗМІСТ

Стан кібербезпеки в Україні ..... 4
Національна система кібербезпеки ..... 9
Кібервійна проти України ..... 10
Боротьба з кіберзлочинністю в Україні ..... 14
Міжнародне співробітництво у галузі кібербезпеки ..... 21
Коронавірус COVID-19 та питання кібербезпеки ..... 26
Світові тенденції в галузі кібербезпеки ..... 32
Сполучені Штати Америки ..... 46
Країни ЄС та Великобританія ..... 52
Китай ..... 57
Російська Федерація та країни ЄАЕС ..... 63
Австралія ..... 65
Інші країни ..... 71
Кібервійни та протидія зовнішній кібернетичній агресії ..... 72
Кіберзахист критичної інфраструктури ..... 77
Захист персональних даних ..... 81
Кібербезпека Інтернету речей ..... 106
Кіберзлочинність та кібертерроризм ..... 108
Діяльність хакерів та хакерські угруповування ..... 146
Вірусне та інше шкідливе програмне забезпечення ..... 152
Операції правоохоронних органів та судові справи проти кіберзлочинців ..... 206
Технічні аспекти кібербезпеки ..... 213
Виявлені вразливості технічних засобів та програмного забезпечення ..... 216
Технічні та програмні рішення для протидії кібернетичним загрозам ..... 246

**«Компанія GigaCloud повідомляє, що першою з українських хмарних операторів отримала на свій дата-центр сертифікат відповідності стандарту інформаційної безпеки PCI DSS. Сертифікацію проводила компанія IT Specialist.**

Гроші на банківській картці – найбажаніша ціль для шахраїв у всьому світі. Щоб гарантувати захист конфіденційних даних клієнтів, компанії мають відповідати стандарту PCI DSS, розробленому провідними міжнародними платіжними системами. Він ставить жорсткі вимоги до захищеності компонентів IT-інфраструктури та цілісності платіжної системи.

«В Україні працюють десятки тисяч організацій, які напряму взаємодіють з даними клієнтських платіжних карток, – каже співвласник GigaCloud та директор з розвитку бізнесу GigaGroup Антон Хвастунов. – Самостійне проходження сертифікації за стандартом PCI DSS може зайняти у них кілька років. Якщо ж компанія розміщується в хмарі або дата-центрі з PCI DSS, термін аудиту та вартість організації належного рівня захисту даних і його підтримка зменшуються в рази».

«До проходження сертифікації компанії GigaCloud та GigaCenter вже мали міжнародні сертифікати з інформаційної безпеки ISO 27001. Це допомогло пройти аудит за PCI DSS в найкоротші терміни, – каже CTO GigaCloud, Кирило Науменко, – Відтепер у наших клієнтів є можливість розміщуватися одразу на двох технічних майданчиках, сертифікованих за цим стандартом: у дата-центрах GigaCenter та BeMobile». ***(GigaCloud та GigaCenter пройшли сертифікацію PCI DSS // Компьютерное Обозрение (https://ko.com.ua/gigacloud_ta_gigacenter_projshli_sertifikaciyu_pci_dss_137566). 02.06.2021).***

***

**«Уряд на засіданні 16 червня ухвалив концепцію реалізації проєкту «Президентський університет».**

Про це повідомляє пресслужба Міністерства освіти й науки України.

Проєкт має започаткувати взірцеву модель інноваційного освітньо-наукового хабу. Його формат дозволить виявити й подолати обмеження для ефективної діяльності закладу вищої освіти, внести, за необхідності, зміни до нормативно-правових актів.

Метою проєкту є створення університету, що поєднує високоякісну освіту, сучасні дослідження та інноваційну діяльність шляхом інтегрування з академічною наукою високого рівня, високотехнологічними компаніями (концепція "трикутника знань").

Концепція передбачає досягнення таких стратегічних цілей:

– створення інноваційного університету згідно з концепцією "трикутника знань" для здобуття перспективної вищої освіти талановитою молоддю;

– забезпечення інноваційного бізнесу, наукових установ та державних органів молодими фахівцями найвищого рівня, запобігання відтоку молодих та перспективних українців за кордон;

– розвиток взірцевого університету, який створюватиме нові національні стандарти навчання та досліджень, освітнього простору та співпраці з науковою сферою та високотехнологічним бізнесом.

«Місія університету в тому, щоб стати моделлю здійснення глибинних реформ у системі вищої освіти і науки України, інноваційним і науковим центром, який забезпечує підготовку високопрофесійних фахівців», – зауважив міністр освіти і науки України Сергій Шкарлет.

Перевагами університету мають стати законодавчо закріплена академічна свобода й інституційна автономія, міжнародний склад викладачів і науковців, залучення до викладання значної кількості фахівців з неакадемічної сфери – бізнесу, державного управління тощо.

Для координації діяльності центральних органів виконавчої влади та реалізації проєкту утворено робочу групу, а в структурі Українського інституту науково-технічної експертизи та інформації – окремий структурний підрозділ – "Центр спеціальних проєктів".

31 травня 2021 року президент України Володимир Зеленський підписав указ про створення президентського Університету інформаційної та кібербезпеки. Навчальний рік в ньому стартує 1 жовтня 2023 року, заявив міністр освіти і науки Сергій Шкарлет.

За його словами, будівництво «Президентського університету» на території державного «Експоцентру України» (ВДНГ, Київ) за три роки обійдеться в 7,2 млрд грн». ***(Кабмін затвердив концепцію проєкту «Президентський університет» // Информационное агентство ЦК, «Эксперт-Центр» (http://expert.org.ua/politika/2021/kabmin-zatverdiv-koncepciyu-proiektu-prezidentskiy-universitet). 17.06.2021).***

***

**«В Киеве в формате онлайн состоялся Форум кибербезопасности для государственного и энергетического сегментов, в ходе которого состоялись презентации новых решений, панельные дискуссии и демонстрация реальных кейсов противодействия кибератакам в ходе киберполигона.**

В основном, все прошло гладко, поскольку организаторы уже имеют опыт в проведении подобных мероприятий. Но во время первых докладов, несмотря на разрешение Full HD трансляции в YouTube, было низкое качество картинки, на что жаловались многие зрители. Зато киберполигон демонстрировался в Zoom, и здесь все было в полном порядке.

Как отметил Мирослав Бондарь, директор департамента Bakotech, организатора конференции, подобное мероприятие проводится не впервые. В прошлом году был проведен форум для финансовой отрасли Украины и, анализируя результаты, количество просмотров, отзывы участников, было решено продолжать такой формат. Поскольку явно ощущается спрос на него, а характерной чертой данного формата является то, что он создан как площадка для обсуждения наиболее актуальных тем вызовов и проблематики кибербезопасности в отдельно взятых отраслях.

«В государственном секторе подобных вопросов и вызовов хватает. Это и создание системы защиты критической инфраструктуры Украины, подготовка квалифицированных специалистов и технологическое оснащение, и конечно же вопросы взаимодействия, внедрение современных стандартов и многое другое», – отметил представитель Bakotech.

«Кибербезопасность приобрела глобальный характер в современном мире. Кибератаки становятся все сложнее и масштабнее. Как свидетельствуют отраслевые исследования, в 2020 году 99% организаций в мире пережили атаки с использованием мобильных вирусов, в связи с распространением дистанционной модели работы во время пандемии COVID. Еще более тревожным признаком является то, что согласно с недавним исследованием McAfee и Центра стратегических и международных исследований, киберпреступления стоили мировой экономике более 1 триллиона долларов – более 1% мирового ВВП», – сказала Илона Штром, атташе по вопросам торговли Американской коммерческой службы в Украине Посольства США. – Соединенные Штаты и Украина одинаково сталкиваются с мощными угрозами в киберпространстве, что создает возможности для сотрудничества. Начиная с первого совместного события в 2017 году, мы укрепляем наше сотрудничество в отрасли кибербезопасности для устранения этих угроз, и, надеюсь, будем вместе пользоваться всеми преимуществами киберпространства”.

По ее словам, на сегодня США вложили в поддержку кибербезопасности Украины более 15 миллионов долларов – преимущественно в виде оборудования, услуг по обучению и т.д. Этот подход охватывает разные государственные учреждения США, которые тесно сотрудничают с широким кругом ключевых партнеров в Украине. Проекты нацелены на оценку уязвимости, проведение обучения по кибергигиене и построение мощной киберинфраструктуры.

«Еженедельно Государственный центр киберзащиты обнародует статистику по атаках. По сравнению с прошлым годом в целом количество атак увеличилось. Констатируем факт увеличения фишинга. Используется верхнеуровневый человеческий фактор. Это элементы проникновения через социальную инженерию, через непоследовательность действий администраторов систем, которым мы напоминаем постоянно, даем рекомендации об обновлениях уязвимостей информационных активов, которые они используют. К сожалению, такой человеческий фактор позволяет киберпреступникам проникать в систему, и, соответственно, эксплуатировать определенные уязвимости. Поэтому мы принимаем меры по максимальному обмену информации о киберинцидентах, вопросами установления сенсоров и сбора телеметрии для ее анализа и выдачи соответствующих рекомендаций», – отметил Андрей Кузмич, начальник Государственного центра киберзащиты Государственной службы специальной связи и защиты информации Украины.

«Мы наблюдаем уже не первый год, и количество атак в принципе кардинально не изменилось. Изменилось их качество. Видимо, наши оппоненты, также как и мы, учатся и если раньше это было аналогом холодных звонков в бизнесе, то сейчас атака приходит через информацию, которая действительно интересна сотруднику, исходя из его функциональных обязанностей. То есть, это

не какая-то реклама, под которую замаскировано негативное воздействие, а это именно то, что необходимо для выполнения служебных обязанностей. И именно этой тенденции в начале перехода в отдаленный режим мы не наблюдали. это мы наблюдаем последние полтора месяца. И с точки зрения противодействия очень сложно расследовать ситуацию. Если раньше на подобную ситуацию тратили примерно два дня работы трех-четырех аналитиков, то сейчас эти затраты увеличились вдвое», – подчеркнул Валерий Ермошин, начальник департамента информационной безопасности НЭК Укрэнерго.

*Киберполигон для отражения кибератак*

Во второй день состоялся так называемый киберполигон, сделанный в формате практической демонстрации возможных кибератак в условиях, приближенных к реальным. Эксперты рассмотрели конкретные кейсы, а также варианты противодействия им. Это атаки по электронной почте, через web, через локальную вычислительную сеть и также через конкретно взятое оконечное устройство.

В создании киберполигона кроме организаторов и компании McAfee, приняли участие специалисты СНБО, а также партнеры с высоким уровнем технической квалификации это из нескольких украинских компаний. Ресурсы же для создания киберполигона были предоставлены датацентром «Парковый». ***(Герман Богапов. Украинский киберполигон продемонстрировал способы противодействия сетевым атакам // Internetua (https://internetua.com/ukrainskiy-kiberpoligon-prodemonstriroval-sposoby-protivodeistviya-setevym-atakam). 03.06.2021).***

***

**«Користувач Joe Biden підписав електронну петицію про відставку заступника голови Офісу Президента Олега Татарова. Як це трапилось – невідомо, однак поставило під питання кібербезпеку цілої держави.**

Підписати петицію на сайті президента можна лише після авторизації через електронний підпис або через Bank-ID. Іншими словами, держава переконується, що петицію підписує реальний громадянин.

Переконується держава в цьому у той самий спосіб, в який робить це при наданні будь-яких адміністративних послуг. Наприклад, коли ви купуєте, продаєте або даруєте нерухомість, створюєте чи продаєте компанію.

В майбутньому на цій системі перевірки буде збудовано онлайн голосування. Спрощено система має такий вигляд.

Ви приходите до кваліфікованого надавача електронних довірчих послуг, який перевіряє по паперових документах, що ви – це реально ви.

Після цього вами видають електронний ключ. Зараз, наприклад, це можна зробити через той самий онлайн-банкінг "Приватбанку", без фізичної присутності у відділенні. Річ у тім, що банк вже знає, що ви – це саме ви, бо ідентифікував вас при відкритті рахунку.

Припустимо, ви вже маєте електронний ключ і хочете отримати адміністративну послугу, наприклад через Дію чи будь-який інший сервіс.

Перше, що ви маєте зробити – верифікуватися там. Відбувається це через державну систему авторизації. Ця система перевіряє дві основні речі:

чи такий електронний підпис справді існує;

чи він справжній, а не, скажімо, тестовий.

Якщо хоча б по одному пункту – мінус, то вас просто не впустить далі. Принаймні мало б не пускати.

*Історія з Joe Biden та Татаровим*

Тепер до самої історії. Пам'ятаєте, як ми у Центрі Протидії Корупції збирали підписи під петицією про відставку заступника Андрія Єрмака – Олега Татарова? Ту петицію підписала людина на ім'я Joe Biden. Англійською.

Знаєте, що це означає? Що, наприклад, хтось з Офісу Президента фальсифікував цей підпис під петицією на своєму сайті. І це найкращий з можливих варіантів.

За гірших варіантів – державна система авторизації пропускає несправжні електронні ключі або справжній електронний ключ було видано на ліву людину. І це ставить під сумнів як захищеність електронного підпису, так і легітимність електронної демократії як такої. Заодно – і всю систему державної кібербезпеки.

*Є 4 варіанти, як підпис міг з'явитися на сайті ОП*

Варіант №1. Підпис зроблено реальним Joe Biden, зі справжніми документами. Відкидаємо його як фантастичний.

Варіант №2. Зімітовано сам факт підпису на сервері петицій. Грубо кажучи, хтось тупо вписав слова "Joe Biden" в табличку підписантів на сайті президента.

Варіант №3. Хтось отримав справжній електронний підпис на підроблені документи Джо Байдена.

Варіант №4. Петицію підписали не справжнім електронним ключем, а ключова державна система авторизації це пропустила.

І якщо варіант з дописуванням Joe Biden прямо на сайті є неприємним, то 2 останні – просто катастрофічні для всієї державної системи надання онлайн послуг. Бо один засвідчує, що в Україні видають справжній електронний підпис на очевидно підроблені документами. Наприклад, підпис ваш, яким "ви" потім, наприклад, подаруєте комусь свою квартиру чи бізнес.

*Діра в IT-інфраструктурі*

Інший варіант засвідчує, що ключова державна система верифікації вважає несправжні електронні ключі – підписами реальних громадян. Для розуміння, тисячі таких ключів генеруються впродовж години.

Держава в смартфоні? Онлайн-голосування на виборах чи, не приведи Боже, референдумах? Ну-ну, ФСБешні хакери в щасливому очікуванні.

Я наголошу, що зараз це вже не про фальсифікацію підпису під петицією, а про діру в ключовому елементі державної IT-інфраструктури. Це проблема зовсім іншого масштабу і наслідків.

*Позиція влади*

Після того, як ми виявили цю проблему, експерти з кібербезпеки цілий день намагалися отримати хоча б якийсь коментар від влади. Проте, і Офіс Президента, і Мінцифри як води в рот набрали.

Коли скандал вийшов з нашого експертного кола в сайти провідних ЗМІ країни, влада була змушена реагувати. Офіс Президента прокоментував, що звернувся до Державної служби спецзв'язку, а остання обіцяла дати вичерпну відповідь найближчим часом.

На момент написання цього блоку від інциденту пройшло 5 днів. П'ять! В світі ІТ – це купа часу. Нагадаю, що несправжні електронні підписи можна генерувати тисячами…». ***(Віталій Шабунін. «Джо Байден» та Татаров: один підпис показав, що кібербезпека України під загрозою // 24 Канал (https://24tv.ua/dzho-baydena-pidpisavsya-pid-petitsiyeyu-tatarova-kiberbezpeka_n1665953). 24.06.2021).***

***

**«У державному концерні «Укроборонпром» з'явиться додаткова посада офіцера з кіберзахисту і кіберзброї. Про це керівник концерну Юрій Гусєв розповів в інтерв'ю виданню «Бабель».**

«Ми ввели посаду директора з інновацій. На першому конкурсі не встановили переможця і зараз шукаємо людину, яка б рухала інновації. Чому? Безпілотні системи, кіберзброя, нові технологічні та високотехнологічні види зброї – це майбутнє, і нам потрібно думати, яким воно повинно бути», – сказав Гусєв.

Він додав, що вважає розвиток нових проєктів і продуктів одним із чотирьох пріоритетів на посаді…» ***(В «Укроборонпромі» з'явиться посада офіцера з кіберзахисту і кіберзброї // MediaSapiens (https://ms.detector.media/kiberbezpeka/post/27580/2021-06-22-v-ukroboronpromi-zyavytsya-posada-ofitsera-z-kiberzakhystu-i-kiberzbroi/). 22.06.2021).***

***

## *Національна система кібербезпеки*

---

**«В Україні скоро з'явиться новий вид військ – кібервійська.**

Про це на зустрічі з радником президента Литви з нацбезпеки Даріусом Кулешюсом заявив секретар Ради нацбезпеки і оборони Олексій Данілов, пише «Я і Закон».

В ході зустрічі Олексій Данілов зазначив, що незабаром в Україні буде утворений новий рід військ – кібервійська.

«Виклики та загрози у кіберпросторі сьогодні набагато небезпечніші, ніж ядерна зброя, і обмін досвідом у цьому питанні є вкрай важливим», — сказав він, додавши, що актуальною у цьому напрямі є активізація співпраці в рамках кіберцентру в Каунасі.

Як повідомляється, Кулешюс підтримав пропозицію про посилення співпраці в сфері кібербезпеки між Україною та Литвою». ***(В Україні створять кібервійська // Я і Закон (https://yaizakon.com.ua/v-ukrayini-stvoryat-kibervijska/). 04.06.2021).***

***

**«Городские системы киберзащиты фиксируют массированную DDOS-атаку на коммунальный дата-центр.**

Об этом сообщает Департамент информационно-коммуникационных технологий Киевской городской государственной администрации.

«Специалисты по кибербезопасности уверяют, что все системы защиты настроены и отрабатывают нагрузки согласно регламенту. Атака может несколько повлиять на скорость и работу киевских сервисов, возможны небольшие перебои в их работе», – говорится в сообщении.

В Департаменте подчеркнули, что все персональные данные пользователей надежно защищены». ***(В КГГА заявили о хакерской атаке на коммунальный дата-центр // LB.ua (https://rus.lb.ua/society/2021/06/09/486660_kgga_zayavili_hakerskoy_atake.html). 09.06.2021).***

***

**«Зловмисники розповсюджують шкідливе програмне забезпечення, що встановлює на комп'ютер користувача віддалений прихований доступ та відправляє документи на підконтрольні їм сервери.**

Хакери на електронні поштові скриньки надсилають листи нібито від імені державних установ, що мають контекст на кшталт: «ви не сплатили податки. Деталі у файлі…», «на вас заведено кримінальну справу. Деталі в додатку…» Інфікування техніки відбувається, коли користувач завантажує архів у додатку листа. Принцип роботи полягає у завантаженні вірусу на комп'ютер користувача для створення віддаленого прихованого доступу та відправлення документів з розширенням.doc,.docx,.rtf та ін. на сервери зловмисників.

Відомо про факти розповсюдження таких листів з використанням нібито електронної поштової скриньки Управління патрульної поліції Києва – kyiv2@patrol.police.gov.ua.

Рекомендації:

– не завантажуйте з Інтернету зашифровані архіви або архіви під паролем. За необхідності зверніться до відправника, аби уточнити, чи був факт відправлення листа із вкладенням. Краще взагалі заблокувати отримання таких файлів через електронну пошту;

– перш ніж відкрити вкладення в електронних листах чи повідомленнях, звертайте увагу на деталі. Краще утриматися від завантаження вкладень електронних листів від сумнівних відправників. Також має насторожити, якщо автор з невідомих причин змінив мову спілкування, тема листа є нетиповою для автора, а також повідомлення, що спонукають перейти за підозрілими посиланнями або відкрити підозрілі файли;

– обмежте можливість запуску виконуваних файлів;

– періодично здійснюйте перевірку системи антивірусом та оновлюйте бази сигнатур;

– використовуйте ліцензійні операційні системи та інше програмне забезпечення, яке періодично оновлюється;

– регулярно здійснюйте резервне копіювання важливих файлів;

– якомога частіше оновлюйте паролі доступу до важливих систем та використовуйте двофакторну автентифікацію.

Якщо ви постраждали від зазначеного правопорушення, звертайтеся до кіберполіції за формою зворотного зв'язку https://ticket.cyberpolice.gov.ua/ або за телефоном: 0800-50-51-70». ***(Кіберполіція попереджає про масовану атаку "вірусу" на державні установи та приватні компанії // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-poperedzhaye-pro-masovanu-ataku-virusu-na-derzhavni-ustanovy-ta-pryvatni-kompaniyi-768/). 03.06.2021).***

***

**«Кіберфахівці СБУ виявили факти цілеспрямованого розповсюдження спецслужбами РФ шкідливого програмного забезпечення. Замовники планували вразити комп'ютерні мережі органів державної влади, місцевого самоврядування та об'єктів критичної інфраструктури.**

Фахівці СБ України встановили, що на початку червня цього року було здійснено масову розсилку електронних листів із підміною адреси відправника. Повідомлення, зокрема, нібито від Управління патрульної поліції Києва містили шкідливі вкладення і були надіслані на адреси низки державних установ.

Шкідливе програмне забезпечення ініціює встановлення клієнтської частини програми (засіб віддаленого адміністрування) на уражений комп'ютер. Це дає можливість іноземній спецслужбі віддалено здійснювати повний контроль над ПК. Встановлено контрольно-командні сервери, які в т. ч. знаходяться на території РФ.

Кіберфахівці СБ України рекомендують провести термінову перевірку інформаційно-телекомунікаційних систем, зокрема використовуючи індикатори, що опубліковані в платформі «MISP-UA» для виявлення їх можливої компрометації та вжиття оперативних запобіжних заходів…» ***(СБУ заблокувала масову кібератаку спецслужб РФ на комп'ютерні мережі українських органів влади // Служба безпеки України (https://ssu.gov.ua/novyny/sbu-zablokuvala-masovu-kiberataku-spetssluzhb-rf-na-kompiuterni-merezhi-ukrainskykh-orhaniv-vlady). 04.06.2021).***

***

**«Протягом тижня з 9 до 15 червня на інформаційні ресурси державних органів було скоєно понад 50 тисяч кібератак, які були успішно заблоковані.**

Про це повідомляє прес-служба Держспецзв'язку.

Зокрема, система захищеного доступу державних органів до мережі Інтернет заблокувала:

50 571 атаку різних видів, що на 17% більше ніж попереднього тижня. Переважна більшість – мережеві атаки прикладного рівня (98%);

19 DDoS-атак. Переважно на вебресурси президента України.

Крім цього, система виявлення вразливостей і реагування на кіберінциденти на об’єктах моніторингу зафіксувала 1 177 118 "підозрілих подій", більшість з яких є спробами отримання прав користувача – 49%, прав адміністратора – 22%, а також по 8% – стосуються порушення корпоративної політики безпеки, підозрілого коду і нестандартних протоколів.

«У разі будь-яких кіберінцидентів, кібератак або підозрілих дій щодо інформаційно-телекомунікаційних систем просимо інформувати урядову команду реагування на комп'ютерні надзвичайні події України CERT-UA», – додали у відомстві». ***(Держспецзв'язку за тиждень заблокувало 50 тисяч кібератак на державні інформресурси // Економічна правда (https://www.epravda.com.ua/news/2021/06/18/675153/). 18.06.2021).***

***

**«За даними кіберполіції України, у 2020 році зафіксували близько 1 мільйона випадків кіберзагроз. Серед них і мережеві атаки, фішинг, DDoS-атаки, поширення шкідливого програмного забезпечення…**

«Упродовж минулого року в Україні зафіксували спроби поширення шкідливого програмного забезпечення через систему електронної взаємодії органів державної влади. Кібератака пов'язана з російським шпигунським хакерським угрупуванням Gamaredon, які також атакували українські установи, військових і правоохоронців, журналістів та різноманітних держслужбовців. Хакери відправляли шкідливу програму шляхом цільового фішингу з прикріпленими шкідливими документами», – йдеться у відповіді відомства.

Зазначається, що в середині минулого року угрупування Gamaredon почали використовувати нові інструменти, які включають модуль для Microsoft Outlook, котрий створює для користувача електронні листи зі шкідливими документами і відправляє їх контактам жертви…». ***(Елена Середа. У кіберполіції нарахували близько 1 мільйона випадків кіберзагроз за минулий рік // Дзеркало тижня. Україна (https://zn.ua/ukr/ECONOMICS/u-kiberpolitsiji-nazvali-najbilshi-kiberataki-v-ukrajini-za-minulij-rik.html). 18.06.2021).***

***

**«Торік хакери намагалися атакувати українські установи мільйон разів, а кожен другий злочин із банківськими картами відбувається за участю співробітників банку, розповів глава Кіберполіції Олександр Гринчак.**

Керівник кіберпідрозділу в інтерв’ю «ZN.ua» пояснив, як змінилася кібербезпека в Україні за кілька років, чому персональні дані українців гуляють по інтернету, а також що думає Кіберполіція про легалізацію криптовалют і як знаходить злочинців, які орудують у даркнеті та Телеграмі. Усе інтерв’ю за хвилину.

Персональні дані українців потрапляють до рук зловмисників через три причини: неграмотність самих людей, які залишають дані в мережі; кібератаки на держоргани і приватні компанії; продаж особистих даних діючими або колишніми співробітниками розпорядників інформації. «Людина попрацював, звільнився, зберіг інформацію і потім її продає».

Найбільша база особистих даних належить державі і вона повинна гарантувати їх збереженість. «Жодній державі у світі не вдається на 100% захистити дані своїх громадян». Зараз ситуація поліпшується і кіберполіція успішно бореться з продажами податкових, митних та інших баз, а також проводить профілактику з адміністраторами, нагадуючи їм про кримінальну відповідальність. У 2020 році до суду відправили десятки подібних справ.

Все більше торговців особистими даними йдуть у даркнет або месенджер Телеграм, що ускладнює їх ідентифікацію або упіймання. Однак «адміністратори цих телеграм-каналів – живі люди, у яких є реальне життя, у якому анонімізація неможлива».

Кіберполіція створила спецпідрозділ, який опікується моделюванням майбутніх злочинних схем в найближчі 5 років. Профільні фахівці з кібербезпеки у відомстві отримують близько 50 тисяч гривень на місяць, у Кіберполіції працює 40 таких експертів.

Глава Кіберполіції не користується сервісом «Дія», тому що «просто ще не встиг» зареєструватися. Але він наполягає, що це «захищений сервіс, я в ньому впевнений на 100%».

Злочини з банківськими картами ростуть з кожним роком. Зловмисники використовують скіммінгові пристрої (накладки на банкомати), крадуть платіжні дані за допомогою шкідливого ПЗ, а також вступають у змову зі співробітниками банків (зазвичай екс-співробітниками). Кожен другий злочин з банківськими картами відбувається за сприяння працівника банку. Кіберполіція активно співпрацює з банками та просить їх підвищити якість внутрішньої безпеки, обладнати банкомати додатковими прихованими камерами, датчиками, програмним забезпеченням, «але просуваємося повільно».

Як захистити банківські картки та платіжні дані від шахраїв: не називати нікому CVV-код на зворотній стороні картки, не говорити відповідь на секретне питання банку, з обережністю підключатися до відкритих Wi-Fi мереж, бо шахраї часто створюють їх фішингові дублікати і отримують доступ до всіх даних на пристрої, в тому числі банківських.

Кіберполіція співпрацює з пенітенціарною службою в боротьбі «тюремними кол-центрами» – ув’язненими, які виманюють через телефонні дзвінки гроші в українців. «За чотири місяці ми вже оголосили підозри 11 особам по 42 епізодам». Про такі схеми знає персонал пенітенціарних установ, але «центральний апарат не замішаний в цьому». Бізнес пропонував свою допомогу по припиненню такої діяльності, але технічне рішення, яке б обмежило дзвінки ув’язнених тільки близькими і родичами, коштує дуже дорого.

Не дуже раціонально витрачати ресурс кіберполіції на приятгнення до відповідальності людей, які розміщують в інтернеті свої відверті фото. Однак кіберполіцейські зобов’язані реагувати на подібні порушення – адже в Україні є відповідальність за порнографію. Припинення публікації порно-контенту не основний вид діяльності кіберполіції. «Велика частина нашої роботи стосується інших речей, що завдають куди більших збитків суспільству, наприклад, хакерських атак».

Міжнародних хакерів складно притягнути до відповідальності через їх транскордонний характер діяльності. «Злочинці перебувають в одних країнах, а злочини скоюють в інших». Однак завдяки партнерству з іноземними колегами зловити кіберзлочинців стає легше. «У нас налагоджена співпраця з іноземними колегами, проходять спільні операції». Сьогодні партнерами української Кіберполіції є правоохоронці з США, Німеччини, Франції, Італії, Польщі, Румунії, Болгарії та інших країн. Нещодавно кіберполіція з США і Південною Кореєю зловили українських хакерів, які шифрували інформацію і вимагали викуп, завдавши збитків на півмільярда доларів.

Українці не йдуть до Кіберполіції, коли стикаються з хакерськими злочинами, тому що «вважають, що звертатися до нас безглуздо, деякі взагалі не знають про Кіберполіцію». Хоча рівень розкриття злочинів у кіберполіцейських росте в середньому на 20-30%.

Україна повинна вдосконалити законодавство в області кібербезпеки. У Раді вже представлені два законопроекти (№4003 і 4004), які наблизять вітчизняну законодавчу базу до реальності і міжнародних стандартів.

Кіберполіція дуже рада легалізації криптовалюти в Україні. «Нам точно було б простіше працювати, якби криптовалюта з'явилася в законодавчому полі», адже сьогодні це основний платіжний інструмент в даркнеті, де продають зброю, наркотики, віруси і різні дані. «Даркнет – це виклик для всіх у світі, але в будь-якому випадку мова йде про живих людей, які десь живуть, кудись ходять, з ким-то спілкуються і користуються телефоном».

У 2020 році хакери намагалися атакувати українські установи мільйон разів. Зараз ситуація з кібербезпекою набагато покращилася з 2017 року, коли країну паралізував вірус Petya. Сайт кіберполіції атакували часто у минулі роки. «Ми справлялися з ними за 15-20 хвилин. Зараз навіть не намагаються». ***(Як персональні дані українців потрапляють до рук злочинців: головне з інтерв'ю керівника Кіберполіції // UA.NEWS (https://ua.news/ua/kak-personalnye-dannye-ukrayntsev-popadayut-v-ruky-prestupnykov/). 24.06.2021).***

***

## *Боротьба з кіберзлочинністю в Україні*

---

**«За допомогою шкідливої програми-вимагача «Clop» фігуранти криптували дані, що знаходилися на інформаційних носіях компаній у Республіці Кореї та США. Надалі за відновлення доступу вимагали гроші.**

Хакерське угруповання викрили співробітники Департаменту кіберполіції спільно з Головним слідчим управлінням Нацполіції. Зловмисники були викриті в рамках міжнародної операції за сприяння та координації Інтерполу (IGCI), та спільно з працівниками правоохоронних органів з Республіки Корея та США.

Встановлено, що шестеро фігурантів здійснювали атаки шкідливого програмного забезпечення типу "Ransomware" на сервери американських та корейських компаній. За дешифрування даних вимагали «викуп», а в разі несплати – погрожували оприлюднити конфіденційні дані потерпілих.

Так, у 2019 році вірусом-шифрувальником “Clop” атакували чотири корейські компанії, в результаті – було заблоковано 810 внутрішніх серверів та персональних комп’ютерів працівників. Хакери розсилали електронні листи зі шкідливим файлом на скриньки працівників компаній. Після відкриття зараженого файлу програма послідовно завантажувала додаткові програми із сервера розподілу та здійснювала повне зараження комп’ютерів жертв віддаленою керованою програмою «Flawed Ammyy RAT».

Використовуючи віддалений доступ, фігуранти активували шкідливе програмне забезпечення «Cobalt Strike», яке надавало інформацію щодо вразливостей заражених серверів для подальшого їхнього захоплення. За дешифровку інформації зловмисники отримали «викуп» у криптовалюті.

У 2021 році фігуранти здійснили атаку та зашифрували персональні дані співробітників і фінансові звіти Медичної школи університету Стенфорда, Університету Меріленду та Університету Каліфорнії.

На відміну від загальних атак-вимагачів, що шифрують велику кількість невстановлених персональних комп’ютерів та серверів, – це атака APT (Advanced Persistent Threat), вона націлена на комп’ютерну мережу конкретної жертви та заражає всю систему за допомогою програми-вимагача.

Загальна сума збитків сягає 500 мільйонів доларів.

Спільними зусиллями правоохоронців вдалося припинити роботу інфраструктури, з якої здійснюється розповсюдження вірусу, та заблокувати канали легалізації криптовалюти, отриманої злочинним шляхом.

Правоохоронці провели 21 обшук у столиці та на Київщині, в оселях фігурантів та в їхніх автівках. До проведення обшуків було залучено підрозділ Тактико-оперативного реагування патрульної поліції. Вилучено комп’ютерну техніку, автівки та близько 5 мільйонів гривень готівкою. На майно зловмисників накладено арешт.

Відкрито кримінальне провадження за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) та ч. 2 ст. 209 (Легалізація (відмивання) майна, одержаного злочинним шляхом) Кримінального кодексу України. Фігурантам загрожує до восьми років ув’язнення. Слідчі дії тривають.

Процесуальне керівництво здійснює Офіс Генерального прокурора України». ***(Кіберполіція викрила хакерське угруповання у розповсюдженні вірусу-шифрувальника та нанесенні іноземним компаніям пів мільярда доларів збитків // Національна поліція. (https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-xakerske-ugrupovannya-u-rozpovsyudzhenni-virusu-shifruvalnika-ta-nanesenni-inozemnim-kompaniyam-piv-milyarda-dolariv-zbitkiv/). 16.06.2021).***

***

**«Житель Херсонської області через розповсюдження шкідливого програмного забезпечення намагався отримати доступ до особистих даних користувачів комп’ютерів.** Нині кіберполіцейські встановлюють кількість потерпілих.

Працівники відділу протидії кіберзлочинам в Херсонській області Департаменту кіберполіції Національної поліції України спільно зі слідчими відділення поліції №2 встановили, що житель області всі хакерські операції проводив з власного будинку. Він самостійно створив шкідливе програмне забезпечення та розповсюджував його у вигляді листів з посиланням. Коли користувачі відкривали посилання, то зловмисник отримував віддалений доступ до комп'ютера потерпілого: зчитував облікові записи, міг змінити пароль та заблокувати доступ дійсним користувачам.

Правоохоронці провели санкціонований обшук за місцем проживання хакера. Вилучили комп'ютерну техніку, за допомогою якої він виходив до мережі Інтернет.

Нині вирішується питання про повідомлення підозри хакеру. Відкрите кримінальне провадження за ч.1 ст.361-1 «Створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин, комп'ютерів» Кримінального кодексу України. Процесуальне керівництво у кримінальному провадженні здійснює Олешківська окружна прокуратура. Зловмиснику може загрожувати до двох років позбавлення волі». ***(Херсонські кіберполіцейські викрили хакера у розповсюдженні шкідливого програмного забезпечення // Національна поліція (https://www.npu.gov.ua/news/kiberzlochini/xersonski-kiberpoliczejski-vikrili-xakera-u-rozpovsyudzhenni-shkidlivogo-programnogo-zabezpechennya/). 10.06.2021).***

***

**«Рада національної безпеки та оборони України ухвалила рішення щодо застосування санкцій до юридичних та фізичних осіб, котрі причетні до розробки компонентів вірусу NotPetya.**

Про це повідомив секретар РНБО Олексій Данілов під час брифінгу 18 червня.

— Це юридичні і фізичні особи, котрі безпосередньо причетні до розробки компонентів вірусу NotPetya. Вони здійснювали його адміністрування, модерацію, організовували кібератаки на об'єкти критичної інфраструктури нашої країни, – зазначив Данілов.

Він додав, що ці кіберзлочинці внесені до санкційних списків США та звинувачуються правоохоронними органами США у межах кримінального процесу через здійснення кібератак на установи США.

*Що відомо про вірус NotPetya?*

Спершу його ідентифікували як Petya.A. Це одна із версій шкідливої програми Petya, яка 27 червня 2017 року масово атакувала комп'ютери.

Цей вірус блокував роботу комп'ютера, а за відновлення роботи вимагав заплатити близько $300 у біткоїнах. Зокрема, в Україні вірусом атакували фінансові підприємства, державні структури, енергетичні та транспорті компанії.

Пізніше про атаку повідомили в РФ, там постраждали такі компанії, як Роснефть, Башефть та Evraz.

Кібератака зачепила низку країн світу: Угорщину, Румунію, Польщу, Італію, Ізраїль, Сербію, Аргентину, Німеччину, Чехію та Румунію. Всього постраждали від вірусу 64 країни, а збитків було завдано на мільярди доларів.

У жовтні 2020 року судова влада США висунула шістьом громадянам РФ звинувачення у комп'ютерних атаках, зокрема, це стосувалося поширення вірусу NotPetya.

Міністерство юстиції США повідомило про шістьох фігурантів справи: Андрієнка Юрія, Детістова Сергія, Фролова Павла, Ковальова Анатолія, Очиченка Артема і Плискіна Петра.

Зазначається, що вони є співробітниками російської розвідки з підрозділу 74455 ГРУ. На думку американських слідчих, цей же підрозділ стоїть за спробами РФ вплинути на результати виборів 2016 року в США». ***(Марія Степанюк. РНБО запровадила санкції проти розробників вірусу NotPetya, які причетні до ГРУ РФ // ФАКТИ. ICTV (https://fakty.com.ua/ua/ukraine/20210618-rnbo-zaprovadyla-sanktsiyi-proty-rozrobnykiv-virusu-notpetya-yaki-prychetni-do-gru-rf/). 18.06.2021).***

***

**«Сотрудник пультовой охранной компании, владеющий продвинутыми навыками работы за компьютером, раздобыл информацию о том, что платежная система ГлобалМани под повышенной нагрузкой начинает работать некорректно.** Высокая частота запросов к серверу компании вызывает нарушения в системе обработки информации (учете средств на балансах кошельков пользователей).

Это приводит к ошибке, когда деньги с кошелька плательщика не списываются, но при этом засчитываются на кошелек получателя. Подобный сбой позволяет добыть деньги буквально «из воздуха». Узнав об этом, хакер разработал план личного обогащения за счет несанкционированного вмешательства в работу информационных ресурсов системы ГлобалМани.

Данная платежная система действует в Украине на основании лицензии на перевод денег, выданной Национальным банком Украины еще в 2013 году. Технически, она представляет собой автоматизированную систему, состоящую из серверного и коммуникационного оборудования, а также облачных сервисов.

ПО, установленное на сервере, обеспечивает проведение операций с деньгами; коммуникационное оборудование обеспечивает обмен данными между серверным оборудованием и объединяет его в распределенный финансовый кластер, масштабирование которого осуществляется при помощи облачных сервисов.

«Кошельки» ГлобалМани – это электронные записи в базе данных платежной системы, которая, в свою очередь, содержит всю информацию о количестве денег, эмитированных системой, а также балансе кошельков всех агентов, торговцев и пользователей системы.

Реализуя свой план, хакер завел кошелек в платежной системе и, пополнив кошелек на 4482,5 грн, при помощи специального вредоносного ПО, передал к серверу ГлобалМани одновременно 23 ложных запроса на вывод 4,4 тыс. гривен на

банковскую карту и один успешный. Такое количество запросов вызвало технические проблемы с проведением платежей в платежной системе.

Далее, он направил 17,017 успешных запросов о переводе денег на разные суммы, между 5-ю, принадлежащими ему, кошельками. Это вызвало желаемый эффект: отправляемые деньги не списывались, но при этом, зачислялись на счета-получатели.

Следующим шагом, хакер продолжил грузить сервер запросами на изменение пароля к одному из кошельков, после чего, администрации платежной системы пришлось принудительно отключить сервера, что вызвало аварийную остановку в работе сайта платежной системы.

В результате спланированной диверсии, молодой человек сумел сгенерировать на своих счетах за счет системной ошибки более 51 тысячи гривен, которые успешно вывел на подставную банковскую карту.

Главной зацепкой, которая помогла правоохранителям выйти на след киберпреступника, стали его домашний IP-адрес и MAC-адрес компьютера, зафиксированные системой ГлобалМани. Именно с этих адресов он авторизовался в проблемных кошельках во время проведения атаки. После того, как правоохранители предъявили ему подозрение, молодой человек чистосердечно раскаялся и возместил ущерб.

Рассмотрев личность обвиняемого, суд пришел к выводу, что преступник, совершивший несанкционированное вмешательство в работу компьютерных систем (ст. 361 УК), представляет среднюю угрозу для общества и может быть освобожден от наказания (тюремное заключение на 2 года), при условии, что в течение 2 лет он не совершит новых преступлений, будет регулярно отмечаться в специальном органе пробации и не покинет пределов Украины». ***(Андрей Майданик. Украинец «добыл» 51 тысячу гривен из интернета, но получил 2 года срока // Internetua (http://internetua.com/ukrainec-dobyl-51-tysyacsu-griven-iz-interneta-no-poluchil-2-goda-sroka). 18.06.2021).***

***

**«Таращанский районный суд Киевской области признал виновным студента украинского ВУЗа в создании и продаже вредоносного ПО через мессенджер Telegram…**

В сентябре 2019 года студент Уманского педагогического университета создал вредоносное программное обеспечение, предназначенное для обхода стандартных процедур аутентификации, путем перенаправления пользователей на специальный веб-сайт и несанкционированного получения персональных данных пользователей Интернета.

В дальнейшем, при помощи программы «Telegram Desktop», юный хакер совершил сбыт вредоносного ПО, а именно файл под названием «update_google_chrome.js», пользователю мессенджера «Telegram» за оплату в размере 80 долларов США, полученную на электронный криптокошелек.

Согласно заключению судебной компьютерно-технической экспертизы, проведенной судебным экспертом, на ноутбуке, который был изъят в ходе обыска по месту жительства студента, был выявлен 91 файл, который идентифицируются

антивирусными программами как вредоносное ПО, среди которых был обнаружен файл под названием «update_google_chrome.js».

Действия обвиняемого суд квалифицировал по ч. 1 ст. 361-1 УК Украины (создание с целью сбыта вредоносного программного средства, предназначенного для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров) автоматизированных систем, а также его сбыт).

28 мая 2021 года между прокурором и подсудимым было заключено соглашение о признании виновности. Подсудимый безоговорочно признал свою виновность в инкриминируемом преступлении, в содеянном искренне раскаялся и активно способствовал раскрытию преступления.

Суд утвердил данное соглашение о признании виновности и назначил согласованную сторонами меру наказания в виде штрафа в размере одной тысячи необлагаемых минимумов доходов граждан, что составляет 17000 гривен». ***(Артем Сереженок. Студент создал вредоносное ПО и продал его через Telegram // Internetua (http://internetua.com/student-sozdal-vredonosnoe-po-i-prodal-ego-cserez-telegram). 20.06.2021).***

***

**«Под покровом глубокой ночи, на одну из бензозаправочных станций в Киевской области подъехал автомобиль Hyundai i30. Водитель направил машину к колонке с терминалом самообслуживания и вставил заправочный пистолет в люк бензобака.**

Убедившись, что за ним никто не наблюдает, молодой человек достал ноутбук, подключился к интернету и, получив доступ к программному обеспечению, управляющему терминалом, ввел специальный код, который позволил ему залить в бак 50 литров бензина совершенно бесплатно.

Спустя пару дней, злоумышленник снова посетил эту АЗС посреди ночи, уже на другом автомобиле (Dacia Logan). И снова он повторил действия, которые позволили совершенно безвозмездно заправить в бак 50 литров топлива.

Обнаружив недостачу горючего, администрация АЗС обратилась с заявлением в полицию, которая возбудила уголовное дело №12020110040000004 по статье 185 УК Украины (кража). В ходе расследования была установлена личность подозреваемого, который оказался жителем Киева, работающим в компании, которая разрабатывает системные решения по осуществлению контроля и учета для газо– и нефтехранилищ.

Работая оператором по обработке информации специальной компьютерной системы, разработанной для учета и самообслуживания автозаправочных станций, он превысил служебные полномочия тем, что использовал известные ему параметры бесплатного отпуска топлива.

Курьез заключается в том, что на сайте самой компании, предлагающей информационные системы для АЗС, говорится: «там, где установлено наше контрольно-измерительное оборудование и программное обеспечение, кражи и мошенничество – практически невозможны».

В суде обвиняемый полностью признал вину и объяснил свой поступок стремлением неправомерного обогащения. Он искренне раскаялся в содеянном,

хотя это и не помогло ему ни сохранить работу, ни избежать уголовной ответственности.

Внимательно изучив личность обвиняемого и его карьерный прорыв из айтишника в воры, суд постановил присудить наказание в виде 3 лет лишения свободы. Учитывая искреннее раскаяние, отсутствие прежних судимостей и то, что обвиняемый не состоит на учете нарколога, судья принял решение, что исправление подсудимого возможно без изоляции его от общества. В результате, 3 года тюрьмы были заменены на 1 год испытательного срока». ***(Андрей Майданик. Суд наказал айтишника за взлом софта терминала АЗС и кражу бензина // Internetua (https://internetua.com/sud-nakazal-aitishnika-za-vzlom-softa-terminala-azs-i-kraju-benzina). 14.06.2021).***

***

**«Суд признал виновным студента украинского ВУЗа в создании и распространении вредоносного ПО и обязал заплатить штраф в размере 34000 гривен…**

В августе 2020 года студент Запорожского института экономики и информационных технологий с целью реализации своего преступного умысла, направленного на создание и распространение вредоносного ПО, предназначенного для перехвата паролей и других средств защиты компьютерных программ и компьютерной информации, создал вредоносную программу под названием «Arcane Stealer by Sakari», которую затем продавал на специализированных интернет-сайтах и через мессенджер «Telegram». Денежные средства за продажу программы злоумышленник получал с помощью платежной системы «Qiwi» на свой электронный кошелек.

По результатам проведенной компьютерно-технической экспертизы данное ПО относится к категории «Программа-шпион» и предоставляет удаленный доступ к компьютеру, на который она устанавливается.

9 апреля 2021 года между прокурором и подсудимым было заключено соглашение о признании виновности. Согласно данному соглашению стороны договорились о формулировке подозрения, всех существенных для данного уголовного производства обстоятельств и правовой квалификации действий обвиняемого по ч.1 ст. 361-1 УК Украины (создание с целью распространения и сбыт вредоносных программных средств, предназначенных для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), автоматизированных систем и компьютерных сетей).

Также сторонами было согласовано, что при утверждении соглашения обвиняемому будет назначено наказание в виде штрафа в размере 34000 гривен.

Суд утвердил соглашение о признании виновности. Имущество, изъятое в качестве вещественных доказательств по данному делу (ноутбук, мобильный телефон, банковская карта), было возвращено владельцу». ***(Артем Сереженок. Студент заплатит штраф за создание и распространение вредоносного ПО // Internetua (https://internetua.com/student-zaplatit-shtraf-za-sozdanie-i-rasprostranenie-vredonosnogo-po). 10.06.2021).***

***

**«Зловмисники втрутилися у внутрішню систему одного з українських банків та заволоділи базою із конфіденційними даними понад 100 тисяч клієнтів. За скоєне фігурантам може загрожувати до восьми років позбавлення волі.**

Викрили правопорушників співробітники управління протидії кіберзлочинам спільно зі слідчими Криворізького районного управління поліції.

Двоє місцевих жителів 19-22 років знайшли вразливість у внутрішній системі банківської установи. Таким чином, юнаки несанкціоновано отримали доступ до бази із персональними даними понад 100 тисяч клієнтів банку. Зокрема, там містилися фотографії громадян із паспортами, їхні анкети, де зазначалися відомості про місце роботи, адресу проживання тощо, а також дані про банківські рахунки.

За нерозповсюдження викраденої бази даних фігуранти вимагали від банку «викуп» у розмірі 100 тисяч гривень.

В оселях зловмисників правоохоронці провели обшуки та вилучили комп'ютерну техніку, на якій зберігалися викрадені відомості, а також мобільні телефони, банківські картки та «чорнові» записи. Вилучене направлено на проведення експертиз.

Кримінальне провадження відкрите за ч. 3 ст. 190 (Шахрайство) Кримінального кодексу України. Санкція статті передбачає покарання у вигляді позбавлення волі на строк від трьох до восьми років. Досудове розслідування триває.

Процесуальне керівництво здійснює Криворізька центральна окружна прокуратура». ***(Кіберполіцейські викрили двох жителів Кривого Рогу у зламі бази даних клієнтів банку // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpoliczejski-vykryly-dvox-zhyteliv-kryvogo-rogu-u-zlami-bazy-danyx-kliyentiv-banku-2461/). 11.06.2021).***

***

## Міжнародне співробітництво у галузі кібербезпеки

**«Як ЄС може допомогти Києву захиститися від масштабних кібератак на критичну інфраструктуру?**

Україна стала сьомою державою серед нечленів Євросоюзу, яка має унікальний формат обміну кращими практиками у сфері кібербезпеки. Досі до цього «елітного клубу» належали лише США, Індія, Бразилія, Японія, Південна Корея та Китай.

Що на практиці може винести Україна з кібердіалогу з ЄС? І чи допоможе цей діалог зміцнити наш захист?

*Збільшення ризиків*

3 червня відбулися перші кібердіалоги Україна – Європейський Союз. Для їх проведення офіційним Києву та Брюсселю знадобилося менше року.

Цей процес було запущено на саміті Україна – ЄС у жовтні 2020 року. У його підсумковій заяві було вперше наголошено на важливості започаткування кібердіалогів.

Ця коротка фраза дала поштовх для підготовки першого засідання кібердіалогів Україна – Євросоюз.

Україна вже тривалий час є об'єктом регулярних і масштабних кібератак, які ставлять під загрозу стабільну роботу критичної інфраструктури. Євросоюз також не є винятком. Лише у 2019 році було зафіксовано 450 інцидентів, пов'язаних із кібератаками на критичну інфраструктуру ЄС та держав-членів, включаючи фінансовий та енергетичний сектори.

Агентство ЄС з питань кібербезпеки (ENISA) опублікувало звіт про кіберінциденти за період 2019-2020 років. З нього випливає, що географія кібернападів постійно розширюється, вони стають все більш досконалими, цілеспрямованими, широко розповсюдженими, все складніше стає ідентифіковувати замовників.

Також збільшується кількість спаму та цільових атак на платформах соціальних медіа. У грудні минулого року хакери атакували Європейське агентство з лікарських засобів та отримали доступ до документів щодо вакцини Pfizer/BioNTech, які зберігалися на сервері Агентства.

Така ситуація значно збільшує потребу Євросоюзу в посиленні співпраці з міжнародними партнерами.

*Перші кроки України*

Україна вийшла на перший раунд кібердіалогів, маючи професійно сформовані інституційні спроможності та необхідну законодавчу базу.

Кібербезпека визначена одним із пріоритетів у системі національної безпеки України.

У березні 2021 року РНБОУ схвалила проєкт нової Стратегії кібербезпеки України на 2021-2025 роки, який дозволить значно зміцнити вже існуючі інституційні спроможності з протидії кіберзагрозам.

Утворено підрозділи забезпечення кібербезпеки або кіберзахисту в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Міністерстві внутрішніх справ, Національному банку, Міністерстві інфраструктури, Міністерстві оборони (Збройних силах України).

З'явився новий потужний актор – Міністерстві цифрової трансформації, розбудовується Національна телекомунікаційна мережа, функціонують захищені центри обробки даних (дата-центри), розпочато функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки.

Для покращення координації діяльності суб'єктів забезпечення кібербезпеки було утворено робочий орган Ради національної безпеки і оборони України – Національний координаційний центр кібербезпеки, рішення якого дозволяють вирішувати найскладніші проблеми у цій сфері.

У лютому цього року Кабінет міністрів запустив Національний центр резервування державних інформаційних ресурсів як експериментальний проєкт.

Вже звичною практикою стало проведення кібердіалогів з іноземними партнерами, однак діалоги з Євросоюзом стали першим форматом, в якому задіяно одне з найпотужніших у світі міждержавних об'єднань.

*Європейський Союз*

Арсенал Євросоюзу в боротьбі з кіберзагрозами є вражаючим.

Перша Стратегія кібербезпеки ЄС прийнята в 2013 році, вона визначала стратегічні цілі та конкретні дії для досягнення кіберстійкості, зменшення кіберзлочинності, розробки можливостей кіберзахисту, розвитку технологічних ресурсів та встановлення послідовної міжнародної політики щодо кіберпростору для ЄС.

Однією з основ нормативно-правової бази ЄС стала Директива 2016/1148 про безпеку мережевих та інформаційних систем, ухвалена у 2016 році.

У тому ж році була презентована Глобальна стратегія зовнішньої політики та політики безпеки ЄС. У розділі "Кібербезпека" зазначається, що стратегічною метою для Євросоюзу залишається посилення інституційних спроможностей інституцій ЄС та держав-членів у протидії кіберзагрозам, при цьому має зберігатися відкритий, вільний та безпечний кіберпростір.

Європейська комісія також прийняла Пакет з кібербезпеки, покликаний забезпечити досягнення трьох цілей: здійснити заходи для забезпечення кіберстійкості, розробити механізм кіберстримування та кібероборони. Підкреслюється важливість створення ефективної кримінально-правової відповідальності за кіберзлочини, для чого має розвиватися міжнародна співпраця.

У 2018 році Європейський парламент увалив резолюцію «Боротьба з кіберзлочинами», в якій зазначається, що Росія і Китай через державні та недержавні інституції займаються плануванням та реалізацією кібератак на критичну інфраструктуру держав-членів ЄС.

Наприкінці минулого року високий представник ЄС Жозеп Боррель оголосив про наміри Євросоюзу створити робочу групу з кіберрозвідки у рамках Центру розвідки Європейського Союзу.

Також було оголошено кілька цікавих новаторських ініціатив, які стосуються партнерів ЄС, включно з Україною. Перше – за участю співробітників Делегацій ЄС в третіх країнах буде створено мережу кібердипломатії. Друге – ЄС планує збільшення надання практичної підтримки партнерам для підвищення їхньої стійкості до кіберзагроз.

*Санкції за кіберзлочини*

Перші кібердіалоги були зосереджені більшою мірою на знайомстві та обміні інформацією про інституційну структуру і повноваження органів у сфері кіберпростору, про останні напрацювання у розробці відповідних політик та законодавчих ініціатив, включаючи оновлення Директиви ЄС про безпеку мережевих та інформаційних систем (Директива NIS), та зусилля України у розробці політик і законодавства у сфері кібербезпеки, узгоджених з правовою та інституційною базами ЄС.

Окрему увагу було приділено координації та співпраці у рамках міжнародних організацій для посилення кіберстійкості і забезпечення відповідальної поведінки держав у кіберпросторі.

У травні 2019 року Рада ЄС ухвалила рішення про запровадження обмежувальних заходів проти осіб та організацій, які здійснюють кібератаки. Таким чином народився новий санкційний режим, який вперше запрацював у 2020 році.

У липні минулого року Рада ЄС прийняла рішення запровадити санкції за здійснення кібератак та іншої шкідливої активності в інтернеті. Російські фізичні особи визнані причетними до вчинення кібератак на ресурси ОЗХЗ (Гаага, Нідерланди) у квітні 2018 року. Щодо них застосована заборона на в'їзд до ЄС, а також заморожування активів.

Головний центр спеціальних технологій Головного управління Генерального штабу МО РФ визнаний причетним до здійснення кібератак NotPetya та EternalPetya. Встановлено, що даний центр відіграє ключову роль у кібердіяльності осередку Sandworm, який здійснив кібератаку на українську енергосистему. У жовтні минулого року Рада ЄС ухвалила рішення щодо запровадження санкцій стосовно двох фізичних осіб та однієї юридичної особи РФ, причетних до кібератаки на федеральний парламент Німеччини.

Формат кібердіалогів створює унікальний майданчик для регулярного обміну інформацією про кібератаки, які здійснюються на критичну інфраструктуру України та Євросоюзу, а також їхніх виконавців і замовників.

Майданчик кібердіалогів має створити для фахівців з України та ЄС унікальні можливості постійної комунікації, оперативного обміну кращими практиками, забезпечити інформування про кіберінциденти та кібератаки на критичну інфраструктуру, які можуть мати спільних замовників ззовні.

Саме з такої співпраці має народитися кіберстійкість – поняття, найбільш популярне сьогодні у Брюсселі, яке повною мірою відповідає національним інтересам України». ***(Андрій Наджос. Кіберстійкість: як досвід ЄС може допомогти Україні // Європейська правда (https://www.eurointegration.com.ua/articles/2021/06/11/7124258/). 11.06.2021).***

***

**«Розпочався процес приєднання України до Об'єднаного центру передових технологій з кібероборони НАТО, який забезпечує боротьбу з кібератаками та кіберзахист інформаційних систем.**

Про це… розповів посол Естонії в Україні Каймо Кууск.

«В результаті недавніх візитів високого рівня в Україну ми почали процес включення України до Об'єднаного центру передових технологій з кібероборони НАТО в Таллінні. На це потрібен час, але початок покладено», – зазначив посол.

У посольстві Естонії в Києві наголосили, що посилення співпраці з Україною у питаннях оборони та інформаційного обміну, зокрема і щодо протидії кіберзагрозам, є одним із пріоритетів уряду Естонії.

«Естонія підтримує зусилля України в побудові потужної системи кіберзахисту і готова поділитися передовим досвідом у цій сфері. Приєднання України до Центру кіберзахисту НАТО поглибить обмін найкращими напрацюваннями з кібербезпеки та сприятиме утвердженню практик

демократичного цифрового урядування в Україні», – йдеться у повідомленні посольства на його офіційній Facebook-сторінці.

На засіданні керівного комітету Центру Естонія висловила свою політичну підтримку Україні у її прагненні наблизитися до стандартів НАТО і готовність сприяти приєднанню України до Центру кіберзахисту.

«Україна зараз на передовій кібердомену та боротьби з викликами в кіберпросторі, тож участь України в роботі Центру кіберзахисту НАТО буде перевагою для всіх нас», – зазначив посол…» ***(Розпочався процес включення України до Центру кіберзахисту НАТО // Європейська правда (https://www.eurointegration.com.ua/news/2021/06/7/7124130/). 07.06.2021).***

***

**«У ЄС вважають Україну «державою на передовій», яка має досвід атак на критично важливу інфраструктуру.**

Європейський Союз і Україна почали діалог з питань кібербезпеки. Про це повідомив глава представництва ЄС в Україні Матті Маасікас в Twitter.

«ЄС веде кібердіалог з дуже небагатьма країнами. Сьогодні почали з Україною – державою на передовій, яке має досвід атак на критично важливу інфраструктуру і чесність виборів. Підтверджуємо нашу загальну прихильність відкритого і безпечного кіберпростору та узгодженню України з правовою / інституційною базою ЄС», – написав Маасікас.

Нагадаємо, в Україні створять президентський Університет інформаційної та кібербезпеки. Навчання в ньому має стартувати 1 жовтня 2023 року. На створення університету витратять 7,2 млрд грн.

Також в РНБО раніше анонсували, що в Україні будуть створювати кібервойска». ***(Україна стала однією з небагатьох країн, з якими ЄС веде діалог із питань кібербезпеки // MEDIASAPIENS (https://ms.detector.media/kiberbezpeka/post/27431/2021-06-03-ukraina-stala-odniieyu-z-nebagatokh-krain-z-yakymy-ies-vede-dialog-iz-pytan-kiberbezpeky/). 03.06.2021).***

***

**«Міністерство закордонних справ України засуджує нещодавні кібератаки проти Польщі, в яких Варшава звинуватила Росію.**

«Україна засуджує нещодавні кібератаки проти Польщі. Висловлюємо солідарність з нашими польськими партнерами і закликаємо міжнародну спільноту об’єднати зусилля у протидії російській агресії проти усього цивілізованого світу», – йдеться в заяві МЗС, оприлюдненій 23 червня в твіттері.

Про те, що польські міністри і депутати зазнали масштабної кібератаки з боку Росії 19 червня заявив прем’єр-міністр Польщі Матеуш Моравецький, посилаючись на інформацію від контррозвідки, Агентства внутрішньої безпеки і союзників.

Його заява пролунала після того, як голова владної партії «Право і справедливість» Ярослав Качинський повідомив про «масштабну кібератаку» на провідних польських політиків, здійснену з Росії.

Качинський додав, що цілями атаки були «вищі чиновники Польщі, міністри, депутати різних політичних сил». ***(Україна засудила кібератаки проти Польщі, в яких звинувачують Росію // Радіо Свобода (https://www.radiosvoboda.org/a/news-ukraina-polshcha-kiberataka/31322792.html). 23.06.2021).***

***

**«Завданням України та Грузії на шляху інтеграції в НАТО є посилення співробітництва у кібербезпеці та сфері безпеки в Чорноморському регіоні.**

Про це заявила Президент Грузії Саломе Зурабішвілі на спільній з Президентом України Володимиром Зеленським пресконференції в Києві, передає кореспондент Укрінформу.

«Наше завдання на шляху інтеграції – посилити сфери співробітництва, і це стосується кібербезпеки, а також безпеки Чорного моря, що буде розглянуто в рамках НАТО», – сказала вона.

Стосовно безпеки в Чорному морі Зурабішвілі акцентувала, що “ми завжди вітаємо, коли кораблі наших партнерів з НАТО заходять у наші порти, і це дуже важливий шлях з боку безпеки».

Президент Грузії наголосила, що на шляху до НАТО дві країни досягли «дуже великого успіху у напряму сумісності».

Вона також привітала заяву саміту Альянсу 14 червня, у якій підтверджується політика відкритих дверей для України та Грузії…». ***(Кібербезпека та Чорне море: Зурабішвілі назвала завдання України та Грузії на шляху до НАТО // Укрінформ (https://www.ukrinform.ua/rubric-polytics/3269348-kiberbezpeka-ta-corne-more-zurabisvili-nazvala-zavdanna-ukraini-ta-gruzii-na-slahu-do-nato.html). 23.06.2021).***

***

## Коронавірус COVID-19 та питання кібербезпеки

**«Увеличение использования облачных сервисов в результате перехода организаций и их сотрудников на удаленную работу из-за пандемии COVID-19 делает корпоративные сети уязвимыми для кибератак.**

Многим компаниям пришлось быстро внедрить работу из дома в начале пандемии, когда сотрудники стали полагаться на облачные сервисы, включая протоколы удаленного рабочего стола (RDP), виртуальные частные сети (VPN) и наборы приложений, такие как Microsoft Office 365 или Google Workspace.

Хотя это позволило сотрудникам продолжать выполнять свою работу за пределами традиционной корпоративной сети, это также увеличило потенциальную поверхность атаки для киберпреступников. Вредоносные хакеры могут использовать сниженный уровень активности мониторинга, в то время как успешный взлом учетных данных, которые используются для удаленного входа в облачные службы, обеспечивает скрытый путь в корпоративную среду.

Исследователи кибербезопасности из компании Zscaler, занимающейся безопасностью, проанализировали сети 1500 компаний и обнаружили сотни тысяч уязвимостей в виде 392298 открытых серверов, 214 230 открытых портов и 60 572 открытых экземпляра облака – все это можно обнаружить в Интернете. В нем утверждалось, что крупнейшие компании имеют в среднем 468 открытых серверов, в то время как крупные компании подвергаются риску 209.

Исследователи определили «открытые» как нечто, к чему любой может подключиться, если обнаружит сервисы, включая удаленные и облачные сервисы. Организации, скорее всего, не подозревают, что эти услуги в первую очередь доступны в Интернете.

В дополнение к этому, исследователи обнаружили непропатченные системы с 202 000 общих уязвимостей и уязвимостей (CVE), в среднем 135 на организацию, при этом почти половина из них была классифицирована как «критическая» или «высокая».

Возможно, киберпреступники смогут обнаружить и использовать эти уязвимости, чтобы проникнуть в корпоративные сети и заложить основу для кибератак, включая кражу данных, программы– вымогатели и другие вредоносные кампании.

«Огромный объем информации, которой делятся сегодня, вызывает беспокойство, потому что все это, по сути, поверхность для атаки. Все, к чему можно получить доступ, может быть использовано неавторизованными или злонамеренными пользователями, создавая новые риски для предприятий, которые не имеют полной осведомленности и контроля об их воздействии на сеть ", – сказал Натан Хоу, вице-президент Zscaler по новым технологиям.

Хотя увеличивающаяся поверхность атаки может повлиять на организации любого размера, международные и крупные работодатели подвергаются наибольшему риску из-за количества сотрудников и распределенной рабочей силы.

Глобальная рабочая сила также может затруднить обнаружение аномальной активности, потому что компания привыкла к сотрудникам, имеющим доступ к сети со всего мира, поэтому злоумышленник не может быть сразу очевиден.

Но можно предпринять шаги, чтобы уменьшить поверхность атаки и, как результат, потенциальный риск для организации. Zscaler рекомендует три шага для минимизации риска корпоративной сети.

Во-первых, необходимо знать свою сеть: зная, какие приложения и службы используются, легче снизить риск. Во-вторых, нужно знать свои потенциальные уязвимости – исследователи рекомендуют, чтобы группы информационной безопасности были в курсе последних уязвимостей и исправлений, которые можно применить для борьбы с ними.

Третье, что следует сделать организациям, – это принять методы, которые минимизируют риск и действуют как сдерживающий фактор для киберпреступников. Например, безопасные учетные данные для облачных служб с многофакторной аутентификацией, поэтому в случае взлома имени пользователя и пароля злоумышленникам не так просто получить доступ к учетным записям и службам.

«Понимая свои индивидуальные поверхности атак и применяя соответствующие меры безопасности, включая архитектуру нулевого доверия, компании могут лучше защитить свою инфраструктуру приложений от повторяющихся уязвимостей, которые позволяют злоумышленникам красть данные, саботировать системы или удерживать сети в заложниках для выкупа», – сказал Хоу». ***(Danny Palmer. Unsecured servers and cloud services: How remote work has increased the attack surface that hackers can target // ZDNet (https://www.zdnet.com/article/unsecured-servers-and-cloud-services-how-remote-work-has-increased-the-attack-surface-that-hackers-can-target/). 16.06.2021).***

***

**«Число атак программ-вымогателей увеличивалось еще до пандемии COVID-19, но распространенность таких кибератак существенно возросла во время пандемии, отчасти из-за дополнительных рисков безопасности, связанных с количеством сотрудников, работающих удаленно.**

По данным компании MonsterCloud, занимающейся кибербезопасностью, количество атак программ-вымогателей во время пандемии увеличилось на 800%. Такое увеличение частоты, вероятно, связано с комбинацией более слабого контроля безопасности в домашних сетях и более высокой вероятностью того, что пользователи будут нажимать на электронные письма-вымогатели на тему COVID-19.

Более того, хотя атаки программ-вымогателей стали более частыми, данные свидетельствуют о том, что они также были более успешными, поскольку многие целевые компании предпочитают платить выкуп, чтобы восстановить свои бесценные данные.

Совсем недавно атака программы-вымогателя Colonial Pipeline, в результате которой был получен выкуп в размере 4,4 миллиона долларов, высветила распространенность, эффективность и разрушительную силу этих кибератак. Проще говоря, как мы и предсказывали, атаки программ-вымогателей стали более распространенными и более дорогостоящими…

Хотя этот тип потери данных и связанное с ним прерывание бизнеса часто защищается специальными полисами киберстрахования, которые могут не содержать требования о «прямой физической потере или повреждении имущества», не все предприятия имеют такие полисы. В результате страхователи могут попытаться возместить потери доходов бизнеса, связанные с программами-вымогателями, обратившись к своим традиционным политикам в отношении собственности, которые действительно требуют предъявления физических потерь или повреждений в качестве предиката для покрытия, в том числе потери дохода от бизнеса.

Вопрос о физической потере или повреждении программ-вымогателей недавно рассматривался Окружным судом США по округу Мэриленд в деле National Ink & Stitch LLC против State Auto Property & Casualty Insurance Co., где компания, занимающаяся вышивкой и трафаретной печатью, столкнулась с вирусом-вымогателем. атака, мешающая ему получить доступ к своим художественным файлам и программному обеспечению. В своем решении в январе

2020 года суд присоединился к растущему большинству голосов по всей стране, установив, что электронные данные, когда они повреждены в результате кибератаки, действительно вызывают требование о физической потере или повреждении имущественной политики.

Однако критически важным для решения National Ink был тот факт, что атака с использованием программ-вымогателей в конечном итоге повредила компьютерную систему застрахованного, поскольку не все данные были восстановлены. Таким образом, хотя застрахованный смог восстановить большую часть своих данных, его компьютерная система была достаточно искажена, чтобы продемонстрировать физическую потерю или повреждение, тем самым открыв возможность для застрахованного лица возместить потерю дохода от бизнеса, вызванную кибер-вторжением.

Но факты National Ink несколько необычны, поскольку застрахованный так и не смог полностью восстановить все свои файлы, и в результате атаки программное обеспечение застрахованного было повреждено, несмотря на то, что застрахованный платил выкуп. В конце концов, примерно 70% организаций, решивших заплатить выкуп, успешно восстанавливают свои данные.

Возникает вопрос, не рассмотренный судом в National Ink: что происходит с точки зрения покрытия, когда выплата выкупа приводит к полному восстановлению данных? Вызывает ли вмешательство и временная неспособность использовать выкупленные данные требование о физической потере или повреждении, предусмотренное традиционными полисами в отношении собственности, и тем самым позволяет застрахованному лицу возместить потерю дохода от бизнеса? Ряд недавних прецедентов, связанных с COVID-19, может пролить свет на эти вопросы.

*Закон о страховании от COVID-19*

За последний год многочисленные суды по всей стране были вынуждены решать один повторяющийся вопрос: являются ли ограничения на использование имущества застрахованным лицом в связи с правительственными постановлениями о закрытии или предполагаемым присутствием COVID-19 физическими потерями или повреждениями в традиционном понимании. политика в отношении собственности, потенциально позволяющая предприятиям вернуть утраченный доход?

Хотя по этому поводу нет полного единодушия, подавляющее большинство судов, рассматривающих этот вопрос, пришли к выводу, что, хотя правительственные ограничения или наличие COVID-19 могут препятствовать использованию имущества застрахованным лицом, возникающая в результате невозможность использовать имущество по назначению не дает. не составлять и не возникать в результате физической утраты или повреждения с точки зрения закона.

Например, в деле Фрэнка Вана Auto Tag LLC против Selective Insurance Co. на юго-востоке компания, занимающаяся передачей права собственности, тегами и регистрацией, временно закрыла свои предприятия в результате приказов о закрытии из-за COVID-19 и стремилась покрыть свои коммерческие убытки. в соответствии с его политикой в области коммерческой собственности, требующей физического ущерба или утраты собственности.

Отвергая аргумент страхователя о том, что он имеет право на страхование, Окружной суд США Восточного округа Пенсильвании в своем заключении от 27 января пришел к выводу, что «должна быть некоторая проблема с физическим помещением, которая препятствует или препятствует коммерческой деятельности» и что «простая потеря возможности функционировать» не является физической потерей или повреждением.

Точно так же в деле Mena Catering Inc. против Scottsdale Insurance Co. компания общественного питания обратилась за страховкой в соответствии с политикой в отношении коммерческой собственности, утверждая, что COVID-19 временно сделал ее собственность «непригодной для использования по назначению и, следовательно, причинил физический ущерб или потерю собственности.

Окружной суд США Южного округа Флориды отклонил этот аргумент, объяснив в решении от 11 января, что «прямая физическая утрата – недвусмысленно требует некоторой формы фактического физического повреждения застрахованных помещений для активации покрытия», но истец «просто не может показать любые такие потери в результате... невозможности доступа к собственному офису». Суд также отметил, что «коронавирус физически не изменяет внешний вид, форму, цвет, структуру или другие материальные размеры собственности».

В деле Pappy's Barber Shops Inc. против Farmers Group Inc. группа парикмахерских требовала покрытия финансовых потерь, понесенных в результате распоряжений о домохозяйствах, связанных с COVID-19, утверждая, что их собственность была сделана «непригодной для проживания или непригодной для жизни». по прямому назначению, «что квалифицируется как физическая потеря».

Опять же, окружной суд США Южного округа Калифорнии не согласился с этим, найдя вместо этого в своем решении от 11 сентября 2020 г., что «убытки от невозможности использования собственности не равносильны «прямой физической утрате или повреждению собственности» в рамках обычных правил. и популярное значение этой фразы и что «физическая утрата или повреждение происходит только тогда, когда собственность подвергается «явным, очевидным физическим изменениям». Суд также отметил, что «временное ухудшение экономически полезного использования собственности "не является «физическая утрата или повреждение».

Наконец, в деле Pez Seafood DTLA LLC против Travelers Indemnity Co. ресторан обратился за страховкой в соответствии с его политикой в отношении собственности, «из-за невозможности использовать собственность для одной из его основных функций – обслуживания обедов в ресторане» во время COVID– 19 пандемия.

Отвергая аргумент ресторана, Окружной суд США Центрального округа Калифорнии в своем заключении от 20 января объяснил, что «для того, чтобы утрата функциональности представляла собой «прямую физическую утрату», должна существовать связь между потерей и физическое изменение или воздействие на помещение или рядом с ним», и что «физическое повреждение» требует «некоторого физического вмешательства, которое ставит под угрозу физическую целостность собственности».

Примечательно, что суд Pez Seafood четко отделил временную потерю, понесенную рестораном-истцом, от постоянной потери данных и искажения системы, о которых шла речь в деле National Ink.

*Применение к потерям от программ-вымогателей*

Итак, как описанная выше судебная практика по коронавирусу может повлиять на доступность или недоступность скрытого кибер-покрытия потерь от программ-вымогателей? В качестве отправной точки мы ожидаем, что страхователи будут утверждать, что эти холдинги должны подтверждать вывод о покрытии. Аргумент, скорее всего, будет заключаться в том, что во время атаки программы-вымогателя программа-вымогатель встраивается непосредственно в данные пользователя, делая данные нечитаемыми и невозвратными до тех пор, пока не будет уплачен выкуп.

Страхователи могут возразить, что это отличает атаки программ-вымогателей от потерь, связанных с коронавирусом, поскольку, хотя суды установили, что «коронавирус физически не изменяет внешний вид, форму, цвет, структуру или другое материальное измерение» собственности, данные, зараженные программами-вымогателями, были изменены. Страхователи также могут попытаться доказать, что это предполагаемое изменение данных, делающее данные нечитаемыми и безвозвратными, является достаточным, чтобы продемонстрировать физическую утрату или повреждение, даже если выкуп уплачен и данные возвращены.

Тем не менее, страховщики могут опровергнуть эти аргументы, указав на заметные параллели, существующие между потерями от COVID-19 и программами-вымогателями. В частности, в каждом из вышеупомянутых случаев коронавируса заявленные потери дохода от бизнеса якобы были вызваны в первую очередь невозможностью использовать собственность. Страховщики в контексте программ-вымогателей приводят аналогичный аргумент; то есть они утверждают, что заявленные ими потери дохода от бизнеса связаны с отсутствием данных, содержащихся в выкупе.

Кроме того, страховщики могут указать на тот факт, что так же, как предполагаемая потеря возможности использования или функции рассматриваемых свойств в вышеупомянутых случаях коронавируса была (в лучшем случае) временной по своему характеру, потери от программ-вымогателей также являются временными. Как только ограничения на коронавирус сняты или пандемия утихнет, имущество застрахованного лица, которое, как утверждал застрахованный, было непригодным для использования, бесспорно, снова становится пригодным для использования для выполнения своей функции до потери.

Тот же аргумент можно привести и в отношении программ-вымогателей, где независимо от того, что данные были временно сделаны нечитаемыми и невозвратными в результате кибератаки, выкуп приведет к восстановлению данных до их потери. В этой связи страховщики могут указать на тот факт, что многие суды пришли к выводу, что требование о «прямой физической утрате или повреждении» предполагает, что это имущество «становится непригодным для будущего использования» или требует «проведения ремонта для его исправления».

Но там, где киберпреступники возвращают выкупленные данные, эти данные должны немедленно работать, и для их использования в будущем не требуется никакого ремонта. Важно отметить, что такая потеря будет отличаться от National Ink, где атака вымогателя навсегда повредила компьютерную систему застрахованного, и не все данные были восстановлены.

Таким образом, как в контексте COVID-19, так и в контексте программ-вымогателей, убыток может быть лучше всего охарактеризован как «временное нарушение экономически полезного использования собственности», что, как показывает судебная практика по коронавирусу, недостаточно для включения покрытия в соответствии с политикой собственности.

Хотя мы ожидаем, что страхователи будут стремиться отличить убытки от программ-вымогателей от потока решений о коронавирусе, обнаружив, что временной неспособности пользоваться собственностью без дополнительных действий недостаточно для доказательства физической утраты или повреждения, параллели не следует игнорировать. Оба случая связаны с потерей дохода от бизнеса, которая в первую очередь вызвана временной невозможностью использовать имущество по назначению. Поэтому мы ожидаем, что богатство прецедентного права, сложившегося во время пандемии, сыграет важную роль в будущих судебных разбирательствах по киберпространству». ***(Thomas Caswell and Peter Kelly Golfman. COVID Rulings May Support Ransomware Insurance Denials // Law360 (https://www.law360.com/articles/1394879/covid-rulings-may-support-ransomware-insurance-denials). 17.06.2021).***

***

## Світові тенденції в галузі кібербезпеки

**«Повышение разнообразия в индустрии кибербезопасности за счет увеличения количества найма людей из разных слоев общества может помочь улучшить онлайн-защиту для всех, потому что это позволит командам по информационной безопасности подумать и защититься от концепций и методов атак, которые они, возможно, не рассматривали раньше.**

Цифры из отчета NCSC о разнообразии показывают, что более 85% профессионалов, работающих в сфере кибербезопасности, являются белыми по сравнению с менее чем 15% из чернокожих, азиатских или смешанных этнических групп.

Две трети отрасли идентифицируют себя как мужчин, по сравнению с 31%, идентифицирующих себя как женщин, в то время как более 84% опрошенных идентифицируют себя как натуралы, по сравнению с 10%, которые считают себя ЛГБТ. Но разнообразие – постепенно – увеличивается.

«Я чувствую, что с точки зрения разнообразия и инклюзивности в индустрии кибербезопасности мы, честно говоря, прошли долгий путь», – сказала ZDNet Security Update Кристин Изуакор, основатель и генеральный директор Cyber Pop-up.

«Определенно есть над чем поработать, но я так рад видеть так много инициатив, направленных на создание разнообразия в отрасли, привлечение большего количества женщин в отрасль, больше цветных людей из всех этих разных слоев общества. Я думаю, это огромно».

Диверсификация отрасли кибербезопасности не только помогает ей лучше отражать население, она может принести различные способы мышления и различные навыки, а также может помочь командам по кибербезопасности получить лучшее представление о том, как злонамеренные хакерские операции они пытаются защищать сети снова работают.

«Люди, которые проводят эти атаки, не смотрят в одну сторону и не имеют разного происхождения. Они происходят из очень разных слоев общества в самых разных частях мира», – объяснил Изуакор.

«Вы не можете защититься от этого, имея один ход мыслей, вам нужны разные точки зрения, вам нужно, чтобы люди, которые защищаются от этих атак, выглядели так же, как люди, которые атакуют, и которые выглядят как разные люди,» она добавила.

Поэтому повышение разнообразия в командах по кибербезопасности должно быть ключевой целью для организаций в отрасли, поскольку это может помочь защитить людей и предприятия от более широкого спектра киберугроз.

«Я искренне верю, что мы не сможем адекватно защититься от атак или разработать решения, методы и вещи, которые нам нужны, если мы будем придерживаться единого мнения – мы должны иметь разнообразие в пространстве, иначе мы потерпим неудачу», – сказал Изуакор.

Также важно понимать, что люди могут идти разными путями к кибербезопасности – некоторые могут получить квалификацию в университете или сертификаты по информационной безопасности, другие могут получить навыки на онлайн-курсах, некоторые могут даже полностью обучиться.

«Важно признать, что у людей разные режимы обучения и разные пути, и это нормально, пока работа выполняется правильно и пока мы защищаемся от этих атак и обеспечиваем большую безопасность», – сказал Изуакор». ***(Danny Palmer. Why improving diversity in cybersecurity is vital for everyone // ZDNet (https://www.zdnet.com/article/why-improving-diversity-in-cybersecurity-is-vital-for-everyone/). 18.06.2021).***

***

**«После двухлетних консультаций Комиссия по финансовым услугам Гернси (Комиссия) опубликовала окончательную форму Правил кибербезопасности (Правила кибербезопасности) и сопровождающее руководство в соответствии с основными регулирующими законами Гернси.** Правила кибербезопасности имеют прямое применение ко всем лицам, имеющим лицензию в соответствии с этими регулирующими законами (Лицензиаты). Прилагаемое руководство (Руководство) предоставляет советам лицензиатов (Совет) примеры того, как лицензиат может удовлетворить требования, изложенные в Правилах кибербезопасности.

*Задний план*

В октябре 2020 года мы опубликовали подробный обзор проекта правил кибербезопасности, который на тот момент был предметом отраслевых консультаций. Отзывы на консультацию были получены от всех секторов промышленности (см. Отчет об обратной связи Комиссии, и «подавляющее большинство» респондентов, как сообщается, поддержали предложения.

После завершения в ноябре 2020 года процесса консультаций 5 февраля 2021 года Комиссия выпустила окончательную форму Правил кибербезопасности с указаниями, опубликованную на ее веб-сайте 15 февраля 2021 года. Правила кибербезопасности вступили в силу 8 февраля 2021 года. и Лицензиаты должны до 9 августа 2021 года внести изменения в свои внутренние средства контроля для обеспечения соответствия.

Согласно исследованию Ponemon Institute по заказу охранной фирмы Keeper Security, «70% финансовых компаний Великобритании пострадали от кибератак в 2020 году» и «более половины (57%) компаний финансового сектора Великобритании считают, что в результате кибератаки становятся все более серьезными. их сотрудников, работающих в удаленных средах». В том же исследовании подчеркивается, что «половина (50%) финансовых компаний Великобритании говорят, что у них до сих пор нет адекватных планов реагирования на киберинциденты».

В таких условиях Правила кибербезопасности являются долгожданным дополнением к дальновидному мышлению и стабильному режиму регулирования Гернси.

*Правила кибербезопасности – обзор*

Правила кибербезопасности остаются без существенных изменений по сравнению с консультационным проектом. Подробности правил кибербезопасности заключаются в следующем:

*Идентифицировать*

Лицензиаты должны убедиться, что они предприняли шаги для идентификации активов (включая данные), которыми они владеют, и для оценки ущерба их бизнесу, если они потеряют доступ к этим активам или если эти активы иным образом стали предметом нарушения кибербезопасности. «Активы» не ограничиваются традиционными ИТ-активами и должны включать системы, людей и активы данных.

Комиссия ожидает, что Правление оценит киберриски, связанные с активами, идентифицированными Правлением, и проанализирует влияние, которое событие кибербезопасности может оказать на целостность, доступность и конфиденциальность этих активов.

*Защитить и обнаружить*

Лицензиаты должны убедиться, что у них есть соответствующие политики и средства контроля для снижения любых выявленных рисков и обеспечения доставки критически важной инфраструктуры во время и после события кибербезопасности.

В Руководстве «средства контроля» подразделяются на следующие категории:

Технический контроль – результатом которых являются меры безопасности, выполняемые или контролируемые через компьютерные системы, такие как инструменты сетевого мониторинга, управление исправлениями, двух– и многофакторная аутентификация, антивирусное программное обеспечение, инструменты защиты электронной почты (фишинг) и управление мобильными устройствами.

Средства контроля людей – которые позволяют сотрудникам выполнять свою работу, а также обеспечивать безопасность бизнеса, например, обучение персонала, тестирование на фишинг и систематическую реализацию программ повышения осведомленности.

Административная политика и средства управления – которые определяют позицию Лицензиата в отношении безопасности. Лицензиаты должны, среди прочего:

• создавать и поддерживать свои политики и процедуры безопасности, чтобы помочь защитить свои данные и другие активы

• при создании политики безопасности помните об основных целях конфиденциальности, целостности и доступности активов.

• проводить регулярные обзоры своих инструментов безопасности, продуктов и услуг, чтобы, помимо прочего, гарантировать, что они остаются пригодными для использования, и обеспечивать надлежащую защиту от рисков, с которыми сталкивается Лицензиат.

• обеспечить, чтобы отчетность Правлению по кибервопросам соответствовала цели и чтобы Правлению предоставлялись значимые данные, касающиеся:

◦ текущие риски кибербезопасности

◦ возникающие риски, угрозы и уязвимости

◦ инциденты и

◦ статус соответствия.

Лицензиаты также должны убедиться, что у них есть соответствующие механизмы для выявления возникновения события кибербезопасности.

*Ответить и восстановить*

Лицензиаты должны иметь возможность продемонстрировать, что у них есть план, направленный на смягчение любых сбоев, вызванных событием кибербезопасности (включая знание и способность продемонстрировать уместность любого группового плана, частью которого может быть Лицензиат). Такая стратегия должна включать планирование восстановления и обеспечение наличия у Лицензиата адекватных резервных копий данных в оперативном и автономном режиме. Если обслуживание или восстановление систем кибербезопасности Лицензиата передается на аутсорсинг третьей стороне, Лицензиат должен иметь возможность продемонстрировать, что он осведомлен о любом плане, принятом этим поставщиком, и что этот план подходит для Лицензиат.

*Требования к уведомлениям*

Лицензиаты должны уведомить Комиссию, когда им станет известно о событии кибербезопасности, которое привело к:

• любая потеря значительных пользовательских данных
• значительная потеря доступности ИТ-систем
• значительные затраты для бизнеса
• значительная потеря бизнес-возможностей, или
• значительная потеря обслуживания пользователей.

Уведомление должно включать следующие сведения, относящиеся к событию кибербезопасности:

• дата, когда это было обнаружено
• дата, когда это произошло
• его природа
• текущие результирующие последствия
• любые возможные последствия в будущем
• действия, предпринятые для смягчения последствий, и
• любые дальнейшие шаги, которые необходимо предпринять.

Выполнение и штрафы за несоблюдение

Поскольку Правила кибербезопасности имеют прямое применение ко всем Лицензиатам, штрафы за несоблюдение установлены соответствующими нормативными законами Гернси, которым подчиняется конкретный Лицензиат.

*Влияние на лицензиатов Гернси*

*Согласие*

Правила кибербезопасности требуют, чтобы у Лицензиата были соответствующие политики, процедуры и средства контроля для снижения риска, связанного с событиями кибербезопасности. Любые политики, процедуры и средства контроля, принятые Лицензиатом, должны отражать Правила кибербезопасности и учитывать Руководство. Правление или его эквивалент несет полную ответственность за соблюдение Правил кибербезопасности.

*Ответить и восстановить*

Комиссия ожидает, что все лицензиаты смогут доказать, что они рассмотрели возможные сценарии сбоев, относящиеся к их бизнесу, которые могут быть вызваны событием кибербезопасности.

*Суждение*

Комиссия признает необходимость использовать суждение при рассмотрении различных вопросов в рамках правил. Например:

• требования в Правилах кибербезопасности часто выражаются как подлежащие соблюдению в соответствии с «размером, характером и сложностью» бизнеса Лицензиата.

• Комиссия может по своему усмотрению исключить или изменить применение любого положения Правил кибербезопасности к конкретному Лицензиату, и

• Комиссия признает определенные пороги существенности, например, в Руководстве отмечается, что внутренняя система защиты от вредоносных программ, блокирующая вирус, не должна автоматически считаться «событием кибербезопасности» (которое, среди прочего, инициирует требование об уведомлении Комиссии).

*Бухучет, ведение учета, делопроизводство*

Когда вы пытаетесь внедрить соответствующие элементы управления, их документирование является ключевым моментом. Все лицензиаты должны иметь возможность предоставить Комиссии доказательства по запросу о том, что Правила кибербезопасности были рассмотрены и внедрены. Комиссия отмечает, что «планы реагирования на инциденты и восстановления могут рассматриваться как отдельные документы или могут быть включены как часть планов обеспечения непрерывности бизнеса и аварийного восстановления Лицензиата».

*Текущий обзор*

Все соответствующие меры, принятые Лицензиатом для соблюдения Правил кибербезопасности, должны пересматриваться как периодически (с интервалами, не превышающими 24 месяцев), так и в ответ на любые триггерные события или события кибербезопасности, и такие проверки должны регистрироваться Лицензиатом.

*Уведомление*

Требования к уведомлению в соответствии с Правилами кибербезопасности дополняют и не предназначены для замены любых отдельных обязательств по уведомлению, которые Лицензиат может иметь в противном случае.

*Обновления руководства после консультации*

По итогам консультации Комиссия внесла в Руководство некоторые дополнения, наиболее интересные из которых приведены ниже:

*Аккредитация*

Комиссия отмечает, что аккредитация от признанного органа, такого как Cyber Essentials, Cyber Essentials Plus или ISO270001, может помочь лицензиату выполнить некоторые требования, изложенные в Правилах кибербезопасности, но одной аккредитации, скорее всего, будет недостаточно для обеспечения полного соответствия..

*Аутсорсинг*

В Руководстве повторяется, что Правление должно поддерживать надзор за любыми операциями, переданными на аутсорсинг, и что Правление сохраняет конечную ответственность за соблюдение Правил кибербезопасности. Сюда входят активы, хранящиеся в облачном хранилище (или аналогичном), которые должны быть четко идентифицированы.

*Рассмотрение*

В дополнение к другим требованиям к отчетности и анализу, изложенным в Правилах кибербезопасности, Совет директоров должен ежегодно отчитываться перед своими акционерами о том, что они довольны своей киберполитикой, средствами контроля и отчетностью.

*Шифрование*

Лицензиатам следует рассмотреть возможность шифрования своих данных, в том числе на съемных носителях и мобильных устройствах, или когда данные отправляются через ненадежную сеть.

*Политики*

Лицензиаты должны учитывать Политику управления доступом в дополнение к другим областям, указанным в Правилах кибербезопасности, как часть их минимальных ожидаемых политик и процедур». ***(Helen Wyatt, Alasdair***

***McKenzie. Guernsey Cyber Security Rules and Guidance // Mourant (https://www.mourant.com/news-and-views/updates/updates-2021/guernsey-cyber-security-rules-and-guidance.aspx). 14.06.2021).***

***

**«Планы правительства Германии разрешить полиции развертывать вредоносное ПО на устройствах любой цели и заставить мир технологий помогать им, как ни странно, натолкнулись на некоторое сопротивление.**

В открытом письме в этом месяце компьютерный клуб Chaos – вместе с Google, Facebook и другими – заявил, что они против предложений о резком расширении использования так называемых государственных троянов, также известных как правительственное шпионское ПО, в Германии. Согласно запланированному законодательству, даже люди, не подозреваемые в совершении преступления, могут быть инфицированы, и поставщики услуг будут вынуждены помочь. Плюс ко всему, всем немецким шпионским агентствам будет разрешено проникать в электронику и средства связи людей.

Эти предложения полностью обходят проблему бэкдора или ослабления шифрования, на которой, похоже, зациклились американские политики. Если у вас есть root-доступ на компьютере или наладоннике, устройство может быть открытой книгой, с шифрованием или без.

«Предложения настолько абсурдны, что все эксперты, приглашенные на заседание комитета в Бундестаге, подвергли их резкой критике», – заявил Chaos.

«Даже Facebook и Google – до сих пор не признанные пионерами конфиденциальности – яростно выступают против проекта. Защитите безопасность и доверие в Интернете – от неограниченного расширения слежки и для защиты шифрования».

*Почему кто-то до сих пор пользуется TikTok?*

TikTok незаметно обновил свои условия и положения, чтобы позволить себе собирать биометрические данные о пользователях, включая «отпечатки лиц и голоса», от пользователей в Соединенных Штатах, а также «определять объекты и декорации, которые появляются, существование и местоположение в пределах изображение черт и атрибутов лица и тела, характера звука и текста слов, произнесенных в вашем пользовательском контенте».

Мы уверены, что сбор данных будет законным в соответствии с законодательством США. Учитывая изобилие законов штатов по этой теме, особенно в Иллинойсе и Калифорнии, это в лучшем случае кажется оптимистичным. Изменения, обнаруженные TechCrunch, вряд ли ослабят непростые отношения между китайским производителем видео-приложений и правительством США.

«Недавно мы обновили нашу политику конфиденциальности, чтобы внести больше ясности в информацию, которую мы можем собирать», – сказал представитель TikTok.

*Федералы: программы-вымогатели – новый терроризм*

Босс ФБР Крис Рэй сравнил продолжающуюся эпидемию программ-вымогателей с атаками 11 сентября 2001 года.

«Есть много параллелей, это очень важно, и мы уделяем большое внимание подрыву и предотвращению», – сказал Рэй Wall Street Journal. «Есть общая ответственность не только между государственными учреждениями, но и частным сектором, и даже средним американцем».

Интервью было проведено после того, как крупнейшая в Америке мясоперерабатывающая компания JBS foods была остановлена с помощью программ-вымогателей, что вызвало опасения по поводу поставок мяса, и через несколько недель после того, как крупный нефтепровод США был вынужден приостановить операции в результате аналогичной атаки.

В среду администрация Байдена распространила коммюнике для бизнес-лидеров, почти умоляя их серьезно относиться к программам-вымогателям. Предлагал обычный совет: патч; разделить сети; регулярно делайте качественные резервные копии в автономном режиме; иметь план восстановления и регулярно проверять его.

*Смартфон родился в США*

Если вы хотите, чтобы смартфон был построен за пределами Китая и огороженных стенами садов Google и Apple, Librem 5 USA от Purism может быть для вас. Librem 5 USA, работающий под управлением PureOS на базе Linux и управляемой пользователем, собирается в стране, и, как и Librem 5, весь исходный код и схемы открыты для изучения и проверки людьми. Плюс есть обычные физические аппаратные переключатели для отключения Wi-Fi, Bluetooth и сотовой связи, а также микрофона и камеры.

Модем Librem 5 USA поступает из Германии (хотя его можно заменить пользователем), а его набор микросхем Wi-Fi – из Индии. Шасси из Китая. Все остальные детали поставляются из США, а сборка устройства производится в Америке. Кажется, что система на кристалле, совместимая с NXP Arm, и другие полупроводники в ней тоже из США.

«Создание Librem 5 USA – это последнее революционное достижение Purism, доказывающее, что не только можно сделать телефон безопасным, избегающим больших технологий, никогда не шпионящим, никогда не отслеживающим, не монополистическим, имеющим выпущенный весь исходный код», и позволяет покупателю фактически владеть им, но также производится в Соединенных Штатах Америки», – провозгласил Purism.

Это оборудование предназначено для людей, которым нужно оборудование, которое не только открыто на уровне схемотехники программного и аппаратного обеспечения, но и построено из цепочки поставок в США. То, что на самом деле внутри чипов, может быть другой историей; это зависит от того, насколько параноиком вы хотите быть.

*Microsoft поглощает ReFirm Labs*

Похоже, что безопасность Интернета вещей вернулась в меню Microsoft, как и должно быть, когда гигант Windows проглотил ReFirm Labs.

Этот стартап стоит за полезным инструментом Binwalk для извлечения прошивки с открытым исходным кодом, который также имеет корпоративную версию. Наряду с CyberX, приобретенным в прошлом году, Microsoft использует технологию ReFirm для Защитника Azure для Интернета вещей.

«Вместе мы продолжим предоставлять нашим клиентам инновации и ценность, помогая им обнаруживать, отслеживать и обновлять все их подключенные к сети устройства», – заявила команда Редмонд. «Технологии и опыт, которые предлагает ReFirm, станут невероятным дополнением к Microsoft и помогут нам продолжать выполнять наши обязательства по защите от чипа до облака». ***(Iain Thomson. Google, Facebook, Chaos Computer Club join forces to oppose German state spyware // The Register (https://www.theregister.com/2021/06/07/in_brief_security/). 07.06.2021).***

***

**«Популярные веб-сайты, включая Twitch и множество новостных сайтов, включая New York Times и Guardian, перестали работать во вторник.**

Другие, включая новостного издателя CNN, сайт социальной сети Reddit и сайт правительства Великобритании gov.uk, также были недоступны. Причина сбоя неясна, но исследователь кибербезопасности Микко Хиппёнен указал на проблемы у Fastly, поставщика облачных услуг, чей собственный веб-сайт также был недоступен.

В 11:58 по брюссельскому времени можно было получить доступ к странице статуса компании, и в ней говорилось о проблеме с ее сетевыми услугами «доставки контента», ссылаясь на сеть центров обработки данных и серверов.

«Проблема была выявлена, и в настоящее время проводится ее исправление», – сказали в компании». ***(PIETER HAECK. Major outage strikes the internet // Politico (https://www.politico.eu/article/major-outage-strikes-the-internet/). 08.06.2021).***

***

**«Сегодня вечером социальные сети были охвачены шумом после того, как тысячи подписчиков HBO Max получили странные электронные письма под названием «Интеграционное письмо №1», в которых в конечном итоге обвиняли стажера HBO Max.**

Электронное письмо, вероятно, было ошибкой разработчика или маркетолога HBO Max, проводившего некоторые тесты на своей платформе, и ошибочно разослал электронное письмо всем подписчикам потоковой сети.

В электронном письме нет ничего особенного, поскольку в нем просто есть тема «Электронное письмо №1 для проверки интеграции» и сообщение, в котором говорится: «Этот шаблон используется только для интеграционных тестов»...

Поскольку тестовое электронное письмо, рассылаемое всем подписчикам HBO Max, было недостаточно, аккаунт HBO Max в Twitter обвинил стажера в ошибочно отправленной рассылке.

Похоже, что в последнее время многие перекладывают вину на стажеров: генеральный директор SolarWinds недавно обвинил стажера в небезопасном пароле «solarwinds123» в производственной среде.

Поскольку HBO Max отправил электронное письмо через Sendgrid, популярную платформу электронного маркетинга, вероятно, это был маркетинговый тест, который по ошибке был проведен для всех зарегистрированных учетных записей HBO Max.

Несмотря на то, что письмо было безобидным, получатели в Твиттере весело проводили время, шутя над письмом HBO Max.

Однако некоторые приняли более серьезные замечания, выразив обеспокоенность тем, что разработчики HBO Max проводили тесты в производственной среде, а не в тестовой». ***(Lawrence Abrams. HBO Max blames mistaken "Integration Test" email on an intern // Bleeping Computer® (https://www.bleepingcomputer.com/news/technology/hbo-max-blames-mistaken-integration-test-email-on-an-intern/). 18.06.2021).***

***

**«Спамеры злоупотребляют партнерскими программами для продвижения онлайн-казино, таких как Raging Bull Casino, Sports and Casino, Ducky Luck и Royal Ace Casino, с помощью вводящих в заблуждение электронных писем.**

Многие крупные онлайн-казино используют партнерскую программу, которая позволяет другим веб-сайтам или влиятельным лицам продвигать свои продукты и зарабатывать комиссию для всех, кто регистрирует учетную запись.

Чтобы направить пользователей, партнеры будут создавать специально созданные URL-адреса, которые содержат идентификатор партнера или удаляют файл cookie, который позволяет казино предоставлять им кредит, когда реферал регистрирует новую учетную запись.

На этой неделе BleepingComputer рассказали об онлайн-спам-кампании, проводимой филиалами онлайн-казино, которые бомбардируют пользователей вводящими в заблуждение электронными письмами, в которых говорится, что они выиграли «Главный приз», что крупная выплата наличными готова или что получатель должен подтвердить свою учетную запись.

После того, как нам рассказали о кампании, мы взглянули на папку со спамом для одной из наших учетных записей электронной почты и увидели, что мы тоже сильно нацелены на эту спам-кампанию…

Хотя Gmail отлично справляется с маркировкой таких писем как спама, другие бесплатные почтовые службы могут не справиться с этой задачей, и спам может попасть в общий почтовый ящик.

Например, ниже приведены два аффилированных спама для казино Raging Bull и казино Royal Ace. Вы можете видеть, что они обещают выплату в размере 3500 долларов, или стратегия ставок будет предоставлена после подтверждения их онлайн-аккаунта.

При нажатии на ссылки пользователь перенаправляется через другой сайт, который сбрасывает партнерский файл cookie, а затем перенаправляет его в казино.

Как вы можете видеть ниже, перенаправление в Raging Bull Casino включает в себя партнерский идентификатор (affid) в URL-адресе, чтобы партнер мог получить кредит за регистрацию.

Как вы можете себе представить, когда вы регистрируетесь в учетной записи, ожидая приятной выплаты, ожидающей вас, выплаты не ждут вас. Вместо этого единственный, кто зарабатывает деньги, – это аффилированное лицо, отправившее вам электронное письмо…». ***(Lawrence Abrams. Watch out: These online casino***

***emails never pay what they promise // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/watch-out-these-online-casino-emails-never-pay-what-they-promise/). 05.06.2021).***

***

**«Программы-вымогатели – одна из самых серьезных проблем в области кибербезопасности, с которыми сегодня сталкиваются организации, но по мере того, как количество заявлений растет, а киберстраховщики смотрят на предлагаемое ими покрытие, могут произойти изменения.**

Киберстрахование предназначено для защиты организаций от последствий кибератак, включая покрытие финансовых затрат на борьбу с инцидентами. Но некоторые критики утверждают, что страхование побуждает жертв программ-вымогателей просто платить выкуп, который затем будет покрыт страховщиками, вместо того, чтобы иметь надлежащую безопасность для сдерживания хакеров в первую очередь. Страховщики утверждают, что решение о выплате выкупа принимает клиент, а не страховщик.

Платить киберпреступникам требование выкупа не является незаконным, но правоохранительные органы предупреждают, что это даст бандам средства для проведения новых атак.

Согласно исследовательскому документу, посвященному киберстрахованию и проблеме кибербезопасности, проведенному оборонным аналитическим центром Royal United Services Institute (RUSI), эта практика не только поощряет киберпреступников, но и не является устойчивой для индустрии киберстрахования, которая предупреждает, что программы-вымогатели стали угроза существованию для некоторых страховщиков.

«На сегодняшний день киберстрахование не оправдало ожиданий, что оно может выступать в качестве инструмента для улучшения практики кибербезопасности организаций», – сказал RUSI. И он предупредил: «Киберстраховщики могут непреднамеренно способствовать поведению киберпреступников, способствуя росту целевых операций с программами-вымогателями».

Программы-вымогатели – одна из самых серьезных киберугроз, с которыми сегодня сталкиваются организации, – как недавно заявила генеральный директор Национального центра кибербезопасности (NCSC) Линди Кэмерон в своем выступлении на RUSI, – поскольку атаки становятся все сложнее и киберпреступники требуют более крупных выкупов.

Отказ платить выкуп может привести к месяцам простоя и огромным расходам для организаций, которые пытаются восстановить свою сеть с нуля – и, согласно RUSI, некоторые жертвы программ-вымогателей и их страховщики заплатят выкуп, потому что они видят в этом вариант с наименьшими затратами. для восстановления сетей.

«Существует широко распространенная обеспокоенность по поводу того, что страховщики подпитывают атаки программ-вымогателей, выплачивая требования о выкупе. Выплата выкупа в настоящее время не является незаконной, и зачастую

дешевле заплатить вымогателям, чем восстановить ИТ-инфраструктуру или покрыть убытки от прерывания бизнеса», – говорится в документе.

Некоторые банды вымогателей даже активно ищут жертв с помощью политик кибербезопасности, потому что они считают, что это лучший способ гарантировать, что они будут зарабатывать деньги на кампаниях по шифрованию.

Однако, согласно отчету RUSI, киберстрахование может фактически сыграть роль в активном разрушении бизнес-модели программ-вымогателей, побуждая держателей полисов улучшать свою защиту, чтобы сделать все возможное, чтобы они не стали жертвами атаки программ-вымогателей. первое место.

В документе предполагается, что страхование должно требовать «минимального контроля над программами-вымогателями» как часть любого покрытия от программ-вымогателей.

Эти средства контроля включают своевременное исправление критических уязвимостей во внешней ИТ-структуре, включение многофакторной аутентификации в службах удаленного доступа, ограничение бокового перемещения путем принятия сегментации сети и внедрения процедур, обеспечивающих создание регулярных резервных копий.

И есть некоторые свидетельства того, что грядут перемены. Согласно недавней статье в Financial Times, страховщики уже увеличивают страховые взносы и предъявляют более строгие требования к стратегиям кибербезопасности, используемым компаниями, которые хотят покупать киберстрахование. The Washington Post также сообщила, что страховщики требуют большой безопасности и сокращают суммы страхового покрытия, которые они готовы предложить.

Все эти рекомендации могут в первую очередь предотвратить атаку вымогателя или уменьшить ущерб, который может нанести атака вымогателя – это означает, что в случае попадания в жертву атаки вымогателя выплата выкупа будет крайней крайней мерой, а не чем быть подписанным как самое простое действие.

Это также снизит риски для индустрии киберстрахования в будущем, уменьшив потребность страховых компаний в поддержке выплат в миллионы долларов за ключи дешифрования после атаки программ-вымогателей.

«Воздействие программ-вымогателей на индустрию киберстрахования подчеркивает необходимость решения некоторых из этих проблем и вопросов раньше, чем позже. Поскольку некоторые страховщики рискуют оказаться в полном объеме из-за убытков, отрасли и правительствам необходимо быстро отреагировать, чтобы обеспечить адекватную защиту и покрытие для предприятий», – сказали исследователи.

Однако, по крайней мере сейчас, доступность киберстрахования, похоже, не способствует повышению кибербезопасности. «Респонденты из правительства, отрасли и бизнеса неизменно заявляли, что положительное влияние киберстрахования на кибербезопасность еще не проявилось в полной мере», – говорится в отчете, добавляя: «Большая часть рынка не использовала ни пряника (финансовые стимулы), ни кнута (обязательства по обеспечению безопасности) для улучшения практики кибербезопасности страхователей». ***(Danny Palmer. Cyber insurance isn't helping with cybersecurity, and it might be making the ransomware crisis worse, say researchers // ZDNet (https://www.zdnet.com/article/ransomware-has-***

***become-an-existential-threat-that-means-cyber-insurance-is-about-to-change/). 28.06.2021).***

***

**«Как мы все знаем, пандемия коронавируса затронула руководителей по информационной безопасности и других лидеров в области безопасности и управления рисками по всему миру. Некоторые из этих руководителей разрабатывают и реализуют проекты безопасности, которые призваны одновременно минимизировать риск и поддерживать удаленных сотрудников.** В разговоре с нашими клиентами они говорят о главных целях на 2021 год, основываясь на уроках, которые мы извлекли из 2020 года.

*Центр управления безопасностью (SOC) Автоматизация*

Первая цель клиента – автоматизация SOC. Многие директора по информационной безопасности говорят об увеличении своих расходов на нетрадиционные меры безопасности, чтобы позволить науке о данных управлять некоторыми из своих мер безопасности. Никто никогда не говорил, что у них достаточно людей для ручного поиска угроз и сортировки всех предупреждений. Это особенно верно в отношении решений безопасности на основе политик, поскольку они генерируют много ложных срабатываний. Таким образом, автоматизация SOC и перепрофилирование команды SOC для более интеллектуального моделирования и расширенного обнаружения угроз – это общая тема, которую мы наблюдали во многих отраслях и регионах.

*Удаленный мониторинг персонала*

Большая часть сотрудников перешла из офисных зданий в разные удаленные места. Одной из проблем, связанных с мониторингом удаленной рабочей силы, является получение информации о ваших данных в режиме реального времени с помощью удаленной рабочей силы, что непросто. Кроме того, важной проблемой является выявление пользователей, склонных к фишинговым атакам. Организациям необходимо идентифицировать пользователей, которые получают доступ к ресурсам из ненадежных или незащищенных мест, потому что теперь они не работают в одном безопасном месте за корпоративным брандмауэром. Сотрудники могут получать доступ к корпоративным активам напрямую через некоторых поставщиков облачных услуг, таких как Microsoft, Amazon или Salesforce, или даже использовать программное обеспечение для виртуальных встреч, такое как WebEx или Zoom. Вы больше не знаете, какие машины подключены к вашим активам. Откуда они на самом деле? А кто откуда подключается? Вам нужно уметь собирать контекст, устанавливать нормальные шаблоны, а затем искать вещи, выходящие за рамки нормы, что является огромной проблемой.

*Аналитика доступа и контроль доступа на основе рисков*

Следующая интересная цель клиента – это аналитика доступа и управление доступом на основе рисков. Из-за пандемии произошло ускорение облачного варианта. Это создало проблемы с точки зрения обеспечения прозрачности рисков доступа. Как вы динамически предоставляете доступ временным сотрудникам? Как вы управляете привилегированным доступом? Проблемы, связанные с обнаружением и очисткой рискованных учетных записей, сертификатами доступа

на основе рисков, а также проверкой подлинности на основе рисков стали критически важной областью для наших клиентов. Особенно сейчас, когда у них так много пользователей, которые входят в систему из разных мест на разных устройствах.

*Обнаружение и предотвращение внутренних угроз*

Следующая важная цель клиента – обнаружение и предотвращение внутренних угроз. Всех беспокоят инсайдерские угрозы, особенно то, что происходит с пандемией. К внутренним угрозам относятся как злонамеренные, так и небрежные инсайдеры. Сюда также входят посторонние, выдающие себя за инсайдеров. Совершают ли инсайдеры мошенничество? Они крадут данные компании? Они смотрят записи, которые им не следует смотреть? Это некоторые из ключевых аспектов, которые наши клиенты хотят знать изнутри. Инсайдерские угрозы бывают разных видов: от шпионажа до кражи, саботажа, мошенничества и конкурентного преимущества. Обычно мы разделяем внутренние угрозы на три основные категории: неправомерное использование доступа, кража данных и компрометация учетной записи или хоста.

*Облачная трансформация*

Следующая цель клиента – преобразование в облако. Мы слышим о преобразовании и внедрении облачных технологий уже несколько лет. И клиенты начали двигаться в этом направлении. В связи с пандемией клиенты, которые планировали преобразование облака через пять лет, сдвинули свои сроки вперед. Ключевая идея заключается в том, что клиенты хотят убедиться, что у них есть безопасный вариант облака. Им нужна прозрачность облачных приложений и инфраструктуры – от Amazon AWS до Azure, Box, Office 365 и т. Д. – а также средства контроля любых угроз в облаке. Они также хотят обнаружить любой привилегированный доступ к облаку, потому что это ключи к их королевству.

*Расширенное обнаружение и ответ (XDR)*

XDR – это новая технология, и клиенты стремятся ее быстро освоить. Одним из ключевых аспектов использования XDR является повышение точности обнаружения угроз за счет объединения всей телеметрии безопасности в организации. Телеметрия конечных точек, сети, приложений и удостоверений интегрирована для обнаружения угроз в реальном времени. Кроме того, XDR обеспечивает более быстрое реагирование на инциденты с быстрой корреляцией инцидентов и их причинно-следственной связью. Автоматические ответные действия запускают сценарии оркестровки и рабочие процессы автоматизации, что в конечном итоге снижает эксплуатационные расходы.

*В заключении*

Что мы узнали из наших инициатив для клиентов, так это то, что работа из дома никуда не денется. Это будет постоянное изменение надолго. Инсайдерские угрозы растут. Автоматизация имеет решающее значение для эффективности SOC. Видимость и безопасность облака важны как никогда. А машинное обучение – это основа для безопасности на основе моделей, которая поможет во всех наших различных инициативах для клиентов.» ***(Saryu Nayyar. Critical CISO Initiatives for the Second Half of 2021 // Threatpost (https://threatpost.com/critical-ciso-initiatives-2021/167309/). 28.06.2021).***

***



**«Президент США Джо Байден отменил и заменил различные распоряжения бывшего президента Дональда Трампа, которые стремились заблокировать такие приложения, как AliPay, TikTok и WeChat, из магазинов приложений в США.**

Когда Трамп делал эти заказы, он назвал китайские приложения угрозой национальной безопасности в отношении информационно-коммуникационных технологий и цепочки поставок услуг.

В соответствии с последней директивой AliPay, CamScanner, TikTok, QQ Wallet, SHAREit, Tencent QQ, VMate, WeChat, WeChat Pay и WPS Office больше не запрещены.

Администрация Трампа распорядилась запретить TikTok, если только он не будет продан американской компании. После нескольких месяцев переговоров после приказа Трампа TikTok заключил предварительную сделку по продаже Oracle и Walmart. Однако, как сообщает The Wall Street Journal, эта сделка была отложена на неопределенный срок после того, как Байден вступил в должность.

Хотя запрет на использование TikTok больше не установлен, в указе не упоминается о потенциальной продаже приложения, которая в настоящее время рассматривается Комитетом по иностранным инвестициям в США.

Новая директива не только заменяет распоряжения Трампа, но и устанавливает новые критерии, которые Министерство торговли должно использовать для проверки того, представляют ли приложения, связанные с иностранными противниками, «неприемлемый риск», согласно информационному бюллетеню Белого дома.

Критерии для определения того, представляет ли приложение «неприемлемый риск», является то, принадлежит ли оно, контролируется или управляется лицами, которые поддерживают военную или разведывательную деятельность иностранного противника, или участвуют в злонамеренных действиях в киберпространстве или связаны с приложениями, которые собирают конфиденциальные личные данные. – говорится в информационном бюллетене.

Указ также предписывает Министерству торговли работать с другими агентствами над выработкой рекомендаций по защите данных потребителей в США от иностранных злоумышленников, а также с рекомендациями относительно дополнительных исполнительных и законодательных мер для дальнейшего снижения риска, связанного с программными приложениями, подключенными к иностранным злоумышленникам». ***(Campbell Kwan. Biden revokes Trump-era executive orders that sought to ban AliPay, TikTok, WeChat // ZDNet (https://www.zdnet.com/article/us-president-biden-revokes-trump-era-executive-orders-that-banned-alipay-tiktok-wechat/). 10.06.2021).***

***

**«Инфраструктура – это одно из тех слов, которые, как нам кажется, мы понимаем, но это может быть трудной концепцией, чтобы осознать это. Мы можем смутно представить себе электрические сети или железные дороги, но инфраструктура также включает в себя множество других услуг, которые необходимы для поддержания процветания наших домов, школ и предприятий.** Она включает дороги и транспорт, телекоммуникационные сети, водопровод и канализацию, а также электричество. И сегодня большая часть этого подключена к Интернету.

«Мы все так глубоко связаны через Интернет, причем разными способами, осознаем мы это или нет», – сказал Джейми Винтертон, директор по стратегии Глобальной инициативы по безопасности Университета штата Аризона. «Было бы ужасно, если бы онлайн-вор украл номер вашей кредитной карты. Но если вода в вашем доме стала небезопасной из-за того, что она была взломана, или если электричество отключилось и сейчас лето в Аризоне или зима на северо-востоке, именно здесь эта связь Интернета с нашей жизнью становится очень прямой, влияя на не только качество нашей жизни, но и источник нашей жизни».

Как недавно напомнили нам взлом Colonial Pipeline и последующее отключение, цифровая связность нашей инфраструктуры, приносящая такие преимущества, как удобство, лучший мониторинг и удаленное решение проблем, делает ее уязвимой для кибератак.

Поскольку администрация Байдена стремится реализовать Американский план рабочих мест, который включает расширение инфраструктуры США, кибербезопасность должна стать ключевым фактором для предотвращения еще более дорогостоящих и опасных атак.

ASU является домом для множества экспертов по кибербезопасности – в областях от информатики и права до бизнеса и гуманитарных наук – которые собираются вместе, чтобы понять и найти решения этой сложной и далеко идущей проблемы.

*Какой у меня стимул?*

Винтертон изучает роль стимулов в кибербезопасности и то, как политика может повлиять на эти стимулы.

«Федеральные законы, касающиеся компьютерного мошенничества, были изобретены в 1984 году», – сказала она. «Компьютеры и Интернет с тех пор значительно изменились, но политикам было очень трудно поспевать за ними».

Одним из результатов этого отставания является трудность определения ответственной стороны. Например, если компания столкнулась с серьезной утечкой данных, виновата ли компания, поставщик программного обеспечения, человек, не исправивший систему, или финансовый директор, не обеспечивший адекватное финансирование безопасности?

Эту путаницу усугубляет тот факт, что кибербезопасность распространяется на несколько федеральных агентств. В этом примере совпадения и пробелы между ними сделают неясным, кто в правительстве должен контролировать расследование утечки данных.

Еще одна нечеткая область – это точное определение последствий утечки данных, например, во сколько это обошлось компаниям и частным лицам.

«Вы точно знаете стоимость, если просчитаете свой автомобиль – это стоимость вашего автомобиля. Но если вы потеряете 145 миллионов кредитных записей, как это произошло с Equifax, какая сумма в долларах назначена на это? Мы действительно не знаем», – сказал Винтертон.

По ее мнению, отсутствие четкой и актуальной политики в конечном итоге означает, что у компаний может быть больше стимулов покупать полис страхования от утечки данных, чем проявлять инициативу в отношении кибербезопасности. Это оставляет данные отдельных лиц недостаточно защищенными.

У людей также могут отсутствовать надлежащие стимулы для разумных действий в области кибербезопасности. Это связано с тем, что при обращении к публике уделяется слишком много внимания всем опасностям и пренебрегают практическими советами, в результате чего люди чувствуют себя подавленными.

«Я всегда спрашивал людей: «Что вас больше всего беспокоит?» Чаще всего я получал ответ: «Не знаю. Я знаю, что мне следует волноваться, но я даже не знаю, о чем беспокоиться», – сказал Винтертон. «И в том случае, как технологи, мы потерпели неудачу. Мы не очень хорошо помогли им понять, в чем заключаются их настоящие угрозы и какие шаги они могут предпринять.

«Если мы переосмыслим законы и политику в отношении кибербезопасности и оценим, какое влияние они на самом деле оказывают, тогда, я думаю, мы начнем видеть, как наши стимулы часто подрывают безопасность. Затем мы сможем понять, как изменить их, чтобы сделать людей, компании и страну более безопасными ».

*Похищение ценных данных*

Представьте, что вы решили стать грабителем. Ваш первый шаг – обойти квартал, пробуя несколько входных дверей, чтобы увидеть, какие из них остались незапертыми.

«Вы можете бегать и делать, может быть, сотню дверей за день, но вы ограничены географией и физикой с точки зрения того, сколько вы потенциально можете проверить», – сказал Адам Дупе. «Если же вы подключите компьютер к Интернету, буквально любой человек на Земле может сказать: «Я собираюсь покачать входную дверь миллиарда устройств в Интернете», и это займет около получаса».

Доупе – исполняющий обязанности директора Центра кибербезопасности и цифровой криминалистики Global Security Initiative и доцент Школы вычислительной техники, информатики и инженерии систем принятия решений. Цель центра – обеспечить безопасность пользователей, независимо от того, работают ли они с iPhone, браузером, электросетью или (гм) нефтепроводом.

«Добавление компьютеров к этим системам часто бывает хорошо, потому что мы получаем большую эффективность, но мы также не думаем о последствиях для безопасности того, что мы делаем», – сказал он.

Критическая инфраструктура представляет собой уникальную проблему кибербезопасности. Поскольку это критично, существует тенденция избегать обновлений безопасности программного обеспечения, поскольку обновление потенциально может испортить другие части системы. По словам Доупе, многие

компании, занимающиеся критически важной инфраструктурой, не имеют процедур, позволяющих проверить, не нарушит ли исправление работу системы.

Злоумышленники часто пытаются использовать эту дилемму, заражая машины до того, как исправление известной уязвимости будет применено ко всем.

Программы-вымогатели – это тип кибератак, при которых хакеры берут данные в заложники, шифруя их и выпуская только тогда, когда владелец данных платит выкуп. Этот тип атаки был причиной временного закрытия Colonial Pipeline и в целом становится все более распространенным.

«Один из рисков, на мой взгляд, состоит в том, что мы настолько сосредоточены на том, чтобы просто предотвратить повторение этого конкретного инцидента, вместо того, чтобы пытаться определить основную причину и применить ее ко всей критической инфраструктуре, которая у нас есть», – сказал он.

Раньше считалось, что программа-вымогатель использовалась против случайных людей и приносила преступнику меньшую сумму в несколько сотен долларов. Однако теперь злоумышленники проводят свои исследования и атакуют ценные данные, которые они могут хранить за миллионы в качестве выкупа.

«Это почти как нападение на детей миллиардеров и их похищение», – сказал Дупе.

Организациям часто говорят, что лучший способ защитить себя от атак программ-вымогателей – это иметь резервные копии данных, которые не подключены к их машинам. Проблема в том, что они не проверяют, насколько быстро они могут восстановить свою систему из резервных копий.

«Мы видели, что если на восстановление у вас уходит месяц, вы платите деньги за программу-вымогатель, даже если у вас есть резервные копии», – сказал Доупе.

Иногда компании думают, что могут ослабить безопасность, если изолируют свои компьютерные системы от общедоступного Интернета и других незащищенных систем, что называется воздушным зазором. Однако преступники по-прежнему могут проникать в сети с воздушным зазором, используя инновационные методы, такие как зараженные USB-накопители, находящиеся поблизости мобильные телефоны и даже звуковые частоты, не обнаруживаемые человеческим ухом.

Это серьезная проблема, иногда со смертельными последствиями, например, когда больница внезапно становится недоступной во время неотложной медицинской помощи, потому что она имела дело с нападением. И поскольку компании продолжают платить эти выкупы, это только вдохновляет все больше киберпреступников требовать их.

Доупе и другие работают над решениями, которые сделают кибербезопасность не такой уж проблемой для крупных компаний.

В настоящее время он участвует в проекте Управления перспективных исследовательских проектов Министерства обороны США по «гарантированному микроплатингу». Они стремятся создать минимально возможный патч (изменяя как можно меньше) и используют математические доказательства, чтобы гарантировать, что система будет продолжать работать после развертывания патча.

По мере того, как США расширяют свою инфраструктуру в соответствии с американским планом рабочих мест, критически важно будет обеспечить кибербезопасность этой инфраструктуры с самого начала, а не пытаться закрепить ее в конце, утверждает Доупе.

*Выбирайте с умом... с помощью ИИ*

Обычно, когда люди думают о безопасности программного обеспечения, они думают о поиске ошибок. Но Тиффани Бао интересуют все решения, которые приходят после момента открытия. Например, когда специалист по кибербезопасности должен сообщить об этом поставщику программного обеспечения безопасности? Когда лучше всего исправить ошибку? Его вообще нужно патчить?

Бао – доцент факультета вычислительной техники, информатики и инженерии систем принятия решений. Она исследует, как бороться с уязвимостями программного обеспечения, сочетая искусственный интеллект и теорию игр, метод, который направлен на поиск лучшего решения по самой низкой цене.

Все действия в области кибербезопасности имеют свою цену – даже хорошо продуманные меры по предотвращению вреда. Например, исправление может вызвать другие проблемы в системе.

«Это похоже на покупку большого предмета мебели. Вы действительно любите его, вы знаете, что он сделает ваш дом красивым, но он огромен. Так что тогда вам нужно подумать, действительно ли вы хотите его купить», – сказал Бао. «Если вы его покупаете, это связано с расходами. За это нужно заплатить, возможно, придется нанять грузчика или поправить другую мебель. Теория игр дает вам прекрасный способ смоделировать затраты и выгоды».

Однако создание модели для поиска оптимальной стратегии может потребовать больших затрат времени и усилий. Здесь на помощь приходит искусственный интеллект – он может дать приблизительные результаты, которые показывают, что с наибольшей вероятностью приведет к оптимальной стратегии. Способность системы находить собственные ошибки и предлагать решения называется кибераавтономией.

Пройдет немного времени, прежде чем кибераавтономные системы будут развернуты; сейчас они все еще находятся в стадии исследований и разработок. Однако Бао и другие исследователи заинтересованы в их понимании и внедрении.

«Если есть система, которая может находить ошибки, а также принимать разумные решения в зависимости от ситуации, то это определенно сделает сеть и компьютер более безопасными», – сказала она.

В настоящее время люди должны выполнять работу по поиску ошибок и выяснению курса действий.

«Люди пытаются принять лучшее решение, но иногда они просто не знают, какое решение будет лучшим», – сказал Бао. Кибераавтономные системы могут лучше вычислить идеальное решение, которое затем они могут представить людям, которые сделают окончательный выбор в отношении того, что им делать.

Теория игр также может предоставить ценную информацию по вопросам, связанным с усилиями в области кибербезопасности, например, об идеальном

бюджете на киберзащиту. Например, модели теории игр могут помочь предсказать результаты с бюджетом в 10 миллионов долларов против 20 миллионов долларов.

«В недавней работе мы обнаружили, что не всегда бывает так, что чем больше бюджета мы выделяем, тем лучше», – сказал Бао. «Вы не хотите тратить слишком много денег, потому что результат не будет таким хорошим, как потратить меньше денег».

Бао видит, что сфера кибербезопасности движется в сторону использования кибераавтономных систем в будущем.

«Мир становится все сложнее», – сказала она. «Нам определенно нужны компьютеры, чтобы помочь нам получить более полное представление и принять правильные решения».

*Как избежать отставания в юридических технологиях*

«Я считаю, что все в Инициативе глобальной безопасности имеет юридический, этический или политический аспект», – сказала Дайана Боуман, изучающая международное управление новыми технологиями. Боуман – профессор юридического колледжа Сандры Дэй О'Коннор и Школы будущих инноваций в обществе, и она часто сотрудничает с Global Security Initiative в своих исследованиях.

Хотя международное управление включает в себя такие вещи, как законы и договоры, большая часть того, на чем фокусируется Боуман, – это то, что она называет мягким правом – не имеющими обязательной юридической силы методами, которые влияют на действия сторон, поощряя определенное поведение. Всемирный экономический форум и Организация экономического сотрудничества и развития – два примера влиятельных лиц, оказывающих влияние на мягкое право.

Мягкое право становится критически важным в регулировании новых технологий, потому что традиционное право не успевает за развитием технологий.

«Когда мы говорим о принятии закона или нового договора, на переговоры могут потребоваться годы. К тому времени, когда вы действительно достигнете соглашения, технология продвинется во многих направлениях. Во многих случаях это не самый эффективный способ регулирования технологии или ее приложений», – сказал Боуман.

С другой стороны, мягкое право более гибкое. Легче добиться, чтобы организация, устанавливающая стандарты, поощряла компании к саморегулированию, создавая своего рода быстрое управление. Даже в этом случае мягкое право по-прежнему отстает, а обеспечение соблюдения более сложное, поскольку больше полагается на стимулы, чем на последствия. Таким образом, не все являются активными сторонниками «мягкого права» как инструмента управления.

Причина того, что и традиционное, и мягкое право в некоторой степени отстают от технологий, заключается в том, что технологическая эволюция идет быстрее, чем когда-либо прежде.

«Кроме того, многие платформенные технологии имеют множество различных приложений в различных сферах. Гораздо труднее не отставать, когда траектория развития технологии менее определена, чем то, что мы видели четыре десятилетия назад», – сказал Боуман.

В качестве примера она приводит нанотехнологии. Когда он был впервые представлен, было трудно представить все его возможные применения. Теперь он используется во всем, от косметики до самолетов, и в нем участвует множество различных регулирующих органов.

Закон о технологиях также сложен, потому что он должен охватывать не только правительства и федеральные агентства, но и частные компании, включая транснациональные корпорации. Но, несмотря на трудности, это становится все более важным. Технологии глубоко встроены в нашу критически важную инфраструктуру, и взлом Colonial Pipeline подчеркивает уязвимость инфраструктуры как с точки зрения кибербезопасности, так и с точки зрения правовых мер. Боуман считает, что в будущем нацеливание на критически важную инфраструктуру станет мощным инструментом для злоумышленников.

«Зарубежной стране намного проще заплатить 10 000 хакеров за нацеливание на критическую инфраструктуру, чем создавать бомбы и развертывать их», – сказала она. «Типы атак, которые мы наблюдали, будут продолжаться, и национальные интересы предполагают, что нам действительно нужно создавать гораздо более проактивные и гибкие решения».

Дипломатия будет играть ключевую роль в будущем, поскольку кибератака может исходить из-за пределов США, ограничивая нашу способность привлечь кого-либо к ответственности. В целом, важно будет лучше понять, как влиять на поведение в отношении новых технологий, таких как международные торговые соглашения.

«Многие люди думают об управлении только с точки зрения возможности привлечь кого-либо к суду, но есть много разных способов, которыми вы можете поощрять или препятствовать поведению», – сказал Боуман. «Это то, о чем мы действительно говорим, когда говорим об управлении».

Задача кибербезопасности слишком сложна для одного человека – или даже для одной академической области – чтобы иметь знания, необходимые для ее решения. Вот почему Global Security Initiative объединяет умы экспертов из всего исследовательского сообщества ASU; проблема, которая затрагивает очень многих, также требует многих точек зрения, чтобы понять ее.

«Подобное исследование будет полезно независимо от того, говорите ли вы о ноутбуке на рабочем столе или о крупномасштабных промышленных системах управления, которые мы видим в инфраструктуре», – сказал Уинтертон». ***(How will we protect American infrastructure from cyberattacks? // Arizona State University (https://news.asu.edu/20210610-solutions-how-will-we-protect-american-infrastructure-cyberattacks). 10.06.2021).***

***

## *Країни ЄС та Великобританія*

**«В Германии кибербезопасность снова находится в центре внимания законодателей.** После отказов ИТ целых университетов и больниц в Германии и поставок топлива в США критические инфраструктуры и компании,

представляющие особый общественный интерес, должны быть привлечены к большей ответственности. Теперь это обеспечивается новым Законом об ИТ-безопасности 2.0 и третьим постановлением «КРИТИС». В столпов поправок являются укрепление Федерального ведомства по информационной безопасности (Bundesamt für Sicherheit в дер Informationstechnik −«BSI») в Законе BSI (BSI-Gesetz «Bsig») и значительное расширение группы обязанных сторон.

Отныне защита потребителей также будет одной из задач BSI. Новая этикетка ИТ-безопасности для потребителей должна четко показывать, соответствует ли продукт соответствующим стандартам ИТ-безопасности. Кроме того, в будущем BSI будет разрешено выполнять сканирование портов на интерфейсах с общедоступными телекоммуникационными сетями некоторых компаний.

Компании должны начать думать о том, какое влияние могут иметь изменения, потому что, в отличие от предыдущих изменений, нет отсрочки или переходного периода, и теперь нарушения могут привести к крупным штрафам до 2 миллионов евро.

Теперь компаниям следует уточнить:

они попадают в расширенную группу обязанных сторон, в частности, как «KRITIS» или «UNBÖFI», и какие требования соответствия ИТ-безопасности они должны выполнять;

они используют критически важные ИТ-компоненты, о которых может потребоваться сообщить в Федеральное министерство внутренних дел (BMI);

необходимо принять меры в отношении их цепочки поставок;

уже существующие процессы могут быть использованы для обеспечения соответствия ИТ-безопасности, особенно в части защиты данных, или при необходимости создания новых процессов; и будет ли

сертификат безопасности ИТ становится необходимым.

Далее мы (1) даем обзор предыстории и наиболее важных изменений. Затем мы более подробно рассмотрим (2) изменения в заинтересованных компаниях и (3) область безопасности продукции и критических компонентов. (4) Наконец, мы обращаем внимание на расширенную компетенцию BSI в области безопасности и надзора за рынком в цифровой сфере.

1. Предпосылки и сфера применения BSIG

Основой для борьбы с угрозами, специфичными для ИТ, такими как кибератаки и инциденты безопасности, является Стратегия кибербезопасности для Германии, Цифровая повестка дня правительства Германии и Директива ЕС о NIS (DIR EU 2016/1148). Эти источники теперь объединены в BSIG.

BSIG поручает BSI, как центральному органу по кибербезопасности, задачи и полномочия, необходимые для обеспечения ИТ-безопасности, как по отношению к федеральным правительственным учреждениям, так и по отношению к частным компаниям. Задачи и полномочия разнообразны и в целом направлены на обеспечение функциональности ИТ-систем, критически важных для государства или функционирования общественной жизни.

Операторы критических инфраструктур («КРИТИС») должны принимать технические и организационные меры для предотвращения нарушений доступности, целостности, аутентичности и конфиденциальности своих

информационных технологических систем, компонентов или процессов. Сюда также входят системы обнаружения атак. Они должны предоставить BSI доказательства того, что эти меры были реализованы. В случае инцидентов безопасности, которые произошли или которых опасаются, необходимо немедленно сообщить о них.

То же самое относится к поставщикам соответствующих цифровых услуг, включая поисковые системы, онлайн-магазины, облачные вычисления и телемедийные услуги.

2. Новые обязанные стороны

Нововведения в области права ИТ-безопасности в первую очередь направлены на расширение группы заинтересованных компаний. В настоящее время термин КРИТИС остается центральным. Это должно быть расширено категорией: удаление бытовых отходов. Регламент определит сферу действия этой категории более подробно.

Категории KRITIS, которые уже были определены и уточнены более подробно, будут дополнительно расширены вторым поправочным постановлением: до сих пор BSIG охватывала приблизительно 1600 операторов критической инфраструктуры. Из-за изменений в соответствующих критериях оценки и пороговых значениях сюда должны быть добавлены около 270 дополнительных операторов.

В дополнении к Kritis, совершенно новая область должны быть включена в каталоге Bsig о обязательствах: Для этого есть теперь новая концепция компании в Особенном Public Interest (Unternehmen им beonderen öffentlichen Interesse − « UNBÖFI »). Таким образом, законодатель хочет принять во внимание тот факт, что ИТ-безопасность важнейших немецких экономических игроков имеет первостепенное значение, даже если они не обслуживают критически важную инфраструктуру (KRITIS). UNBÖFI, по сути, представляют собой компании трех типов, включая их центральных поставщиков :

*Производители продуктов для ИТ-безопасности*

Производители продуктов для ИТ-безопасности являются производителями или разработчиками товаров в значении Раздела 60 (1) п. 1 и 3 Постановления о внешней торговле и платежах Германии (Außenwirtschaftsverordnung). Сюда входят компании, которые:

Производство продуктов с функциями ИТ-безопасности для обработки секретной правительственной информации; или же

Изготовить или изготовить компоненты таких продуктов, которые необходимы для функции ИТ-безопасности, и при этом иметь технологию, на которой она основана;

и их продукты или, в случае компонентов, важных для функции ИТ-безопасности, все продукты были одобрены BSI.

Критические операторы в соответствии с Федеральным законом Германии о контроле за выбросами

Критические операторы в соответствии с Законом о борьбе с загрязнением воздуха немецкого федерального (Bundesimmissionsschutzgesetz − BImSchG) являются те операторы, которые попадают в рабочую зону верхнего класса в

соответствии с 12 – й BImSchV (майор Аварии Regulation), а также те операторы рабочей области более низкие классы, эквивалентные классам, указанным в правилах, т. е. операторы, использующие вещества, обозначенные как опасные, присутствуют в количествах, которые достигают или превышают пороговые значения количества, указанные в правилах.

*Компании, имеющие важное экономическое значение*

Компании, имеющие важное экономическое значение, – это компании, которые входят в число крупнейших компаний Германии с точки зрения добавления стоимости на внутреннем рынке и, следовательно, имеют большое значение для экономики Германии. Тем не менее, какие именно компании подпадают под действие этого правила, еще предстоит определить в дальнейших постановлениях. Указание на возможный список дается в так называемом основном отчете Комиссии по монополиям Федерального управления картелей Германии, в котором перечислены 100 крупнейших компаний с точки зрения их экономической ценности. Текущий отчет можно посмотреть здесь; Список за отчетный 2018 год можно найти в таблицах в главе II.

*Поставщики компаний, имеющих важное экономическое значение*

Поставщики компаний, имеющих важное экономическое значение, которые важны из-за их уникального торгового предложения. Однако то, что подразумевается под «уникальным торговым предложением», также должно быть определено в новом постановлении.

3. Безопасность продукта и важные компоненты

С принятием Закона об ИТ-безопасности 2.0 цифровизация законодательства о продуктах продвигается вперед.

*Идентификатор ИТ-безопасности*

Будет введена добровольная этикетка безопасности ИТ, чтобы информировать потребителей, которые компании могут использовать, среди прочего, в маркетинговых целях. С этой целью BSI представит единую этикетку, чтобы информировать потребителей об ИТ-безопасности продуктов в определенных категориях продуктов, определенных BSI. Этикетка, вероятно, будет представлять особый интерес для иностранных компаний, поскольку она убедит немецких потребителей в том, что ИТ-продукт соответствует немецким стандартам безопасности.

Во исполнение европейского законодательства планируемые поправки к Гражданскому кодексу Германии (Bürgerliches Gesetzbuch − BGB) создадут обновленные обязательства для компании-дистрибьютора в случае предоставления потребителям цифровых продуктов.

*Полномочия BSI по вмешательству*

Дальнейшие поправки касаются создания полномочий вмешательства для BSI при использовании и работе критических компонентов. Постановление, запрещающее использование таких компонентов от ненадежных производителей, предназначено для повышения безопасности продукции в области критических инфраструктур.

Охватывается как аппаратное, так и программное обеспечение, имеющее большое значение для функционирования сообщества, поскольку нарушения

доступности, целостности, аутентичности и конфиденциальности ИТ-продукта могут привести к сбою или значительному ухудшению функционирования критически важных инфраструктур или угрозам общественной безопасности.

Новые требования к критически важным компонентам тесно переплетены с новым Законом о телекоммуникациях. Дополнительные сведения см. В нашем Уведомлении для клиентов о Законе о модернизации электросвязи.

4. В цифровой сфере: безопасность и надзор за рынком со стороны BSI– обязательства компаний

BSIG с поправками также служит для адаптации механизмов защиты и стратегий защиты с учетом постоянного увеличения количества вредоносных программ для ИТ. В частности, он обеспечивает улучшение защиты продуктов и систем ИТ, представленных на рынке, в том числе путем предоставления BSI дополнительных полномочий по тестированию и мониторингу и установления минимальных стандартов:

BSI получил право обнаруживать вредоносные программы. Например, BSI разрешено использовать так называемое «сканирование портов», чтобы определить, закрыли ли операторы общедоступных систем информационных технологий уязвимости безопасности, которые стали известны BSI.

Если BSI узнает об уязвимостях безопасности или рисках, исходящих от телекоммуникационных или телемедийных услуг, орган может приказать поставщикам таких услуг принять меры по устранению рисков (например, обновить программное обеспечение).

Закон о безопасности ИТ 2.0 также дает BSI широкие полномочия по выдаче распоряжений поставщикам телекоммуникационных и телемедийных средств для предотвращения конкретных угроз информационной безопасности. В то же время расширяются и обязательства перед компаниями». ***(Christian Schefold, Julia Pfeil, Sebastian von Haldenwang, Nico Winter, Florian Mörth. The extension of the German IT Security Act: Cybersecurity is now a mandatory duty for many companies // Dentons (https://www.dentons.com/en/insights/articles/2021/june/8/challenges-of-the-new-bsi-law-cyber-security-is-becoming-a-must-for-many-companies). 08.06.2021).***

***

**«Европейская комиссия объявила о планах создания совместного кибер-подразделения для борьбы с крупномасштабными кибератаками.**

Комиссия заявила, что недавние инциденты с программами-вымогателями для критически важных служб в Ирландии и США «сосредоточили внимание».

В нем утверждается, что кибератаки представляют собой угрозу национальной безопасности, поскольку количество инцидентов в Европе выросло с 432 в 2019 году до 756 в 2020 году.

В нем говорится, что специальная группа международных кибер-экспертов будет быстро направлена в европейские страны во время серьезных атак.

Выдвигая предложения, вице-президент Европейской комиссии Маргаритис Схинас заявила, что взлом в прошлом месяце на поставки топлива в США был «кошмарным сценарием, к которому мы должны подготовиться».

В прошлом месяце киберпреступная банда под названием Darkside отключила Colonial Pipeline почти на неделю, что вызвало панические покупки и нехватку топлива.

Хакеры-вымогатели используют вредоносное программное обеспечение для шифрования и кражи компьютерных данных организации, взимая с жертв деньги, чтобы вернуть услуги в нормальное состояние.

Правительство США также недавно сформировало Целевую группу по программам-вымогателям, а Национальный центр кибербезопасности Великобритании предупреждает, что программы-вымогатели являются самой большой киберугрозой для Великобритании.

Европейская комиссия заявила, что продолжающаяся атака программ-вымогателей на службы здравоохранения Ирландии является еще одним признаком того, что кибератаки являются проблемой национальной безопасности.

Управление здравоохранения (HSE) в Ирландии подверглось нападению группы вымогателей под названием Conti, которая взломала ИТ-системы, вызвав серьезные нарушения во многих больницах.

В среду глава HSE Пол Рид сообщил комитету по здравоохранению Oireachtas, что на починку системы уйдут месяцы.

Он сказал, что восстановление будет стоить до 100 миллионов евро (85 миллионов фунтов стерлингов), а также будет связано с большими «человеческими издержками».

Комиссар ЕС по внутреннему рынку Тьерри Бретон заявил журналистам, что группы быстрого реагирования Объединенного кибер-подразделения могли бы помочь Ирландии оправиться от кризиса.

Он сказал, что это подразделение поможет в аналогичных сценариях, «очень быстро развернув специальную команду, что у нас сейчас нет возможностей сделать. Мы знаем, что чем дольше вы ждете, тем хуже, поэтому быстрее и солидарнее вы можете ожидать".

Г-н Бретон настаивал на том, что новое подразделение не будет конкурировать с национальными кибер-организациями или дублировать работу.

Он пообещал создать команду для оказания виртуальной и физической поддержки, используя ресурсы «из одной страны в другую» для оказания оперативной и технической помощи.

Цель состоит в том, чтобы обеспечить функционирование Совместного кибер-подразделения к июню следующего года и его полное создание через год, к 30 июня 2023 года». ***(Joe Tidy. EU wants emergency team for 'nightmare' cyber-attacks // BBC (https://www.bbc.com/news/technology-57583158). 24.06.2021).***

***

## ***Китай***

**«Компания Huawei открыла крупнейший Международный центр по вопросам кибербезопасности и защиты конфиденциальности в г. Дунгуань (Китай).** На церемонии открытия выступили представители GSMA, SUSE,

Британского института стандартов, а также органов государственного контроля из ОАЭ и Индонезии.

Помимо нового центра Huawei представила «Основные принципы кибербезопасности продуктов» (Huawei Product Cyber Security Baseline). Компания впервые обнародует свою базовую концепцию управления безопасностью продуктов для свободного пользования. Открытие центра состоялось в рамках масштабной кампании Huawei по взаимодействию с клиентами и партнерами для совместного укрепления кибербезопасности во всей телекоммуникационной отрасли.

«Вопрос кибербезопасности стоит как никогда остро, — отметил Кен Ху (Ken Hu), ротационный глава совета директоров Huawei, во время открытия центра в городе Дунгуань. — Как представителям одной отрасли нам стоит сотрудничать, обмениваться опытом и развивать наши способности в сферах управления, нормативных актов, технических стандартов и требований. Мы должны дать основания общественности и органам контроля быть уверенными в безопасности продуктов и услуг, которыми они пользуются каждый день. Вместе мы можем достичь необходимого баланса между сетевой безопасностью и развитием в цифровом мире».

Активный перевод бизнеса на цифровые рельсы и новые технологии, такие как 5G и искусственный интеллект, значительно усложнили киберпространство, в частности тем фактом, что из-за пандемии COVID-19 люди проводят большую часть времени в интернете. Эти тенденции привели к росту новых киберрисков.

Компания Huawei открыла новый Международный центр по вопросам кибербезопасности и защиты конфиденциальности в Дунгуане для решения этих рисков. Центр создан с перспективой предоставления платформы заинтересованным сторонам для обмена опытом в киберуправлении и совместной работы над техническими решениями. Он построен с целью демонстрировать найденные решения, способствовать общению внутри отрасли и созданию совместных инноваций, а также предоставлять возможность проводить оценку и сертификацию безопасности. Центр будет открыт для органов контроля, независимых тестирующих организаций, организаций по стандартизации, а также клиентов, партнеров и поставщиков Huawei.

Организации GSMA и 3GPP сотрудничали с заинтересованными сторонами для внедрения единого подхода к кибербезопасности в телекоммуникационной отрасли — стандартизированного механизма оценки кибербезопасности NESAS. Они получили признание игроков отрасли и будут играть важную роль в развитии и проверке сетевой безопасности.

«Предоставление имеющихся и новых технологий в эру 5G будет существенно зависеть от подключения в мобильных сетях, а также надежности и безопасности базовой технологии, — отметил Матс Гранрид (Mats Granryd), генеральный директор GSMA. — Такие инициативы, как «База знаний по кибербезопасности GSMA 5G» (GSMA 5G Cybersecurity Knowledge Base), разработаны, чтобы помочь заинтересованным сторонам понять и сократить сетевые риски. А NESAS, стандартизированный механизм оценки

кибербезопасности, призван способствовать повышению уровня безопасности сетевого оборудования во всем секторе».

Также на мероприятии Huawei представила «Основные принципы кибербезопасности продуктов» (Huawei Product Cyber Security Baseline). Они разработаны в результате более чем десятилетнего опыта компании в отрасли управления безопасностью продуктов, в частности создания ряда внешних нормативных актов, технических стандартов и требований. Вместе с другими механизмами управления Huawei основы помогают обеспечить качество, безопасность и надежность ее продуктов. Отмечается, что за последние годы Huawei построила более 1500 сетей, охватывающих свыше 3 млрд человек в 170 странах и регионах. Ни в одной из этих сетей не выявлены значительные инциденты нарушения безопасности.

«Мы впервые делимся нашими основными принципами со всей отраслью, а не только основными поставщиками, — сказал Шон Ян (Sean Yang), директор глобального отдела кибербезопасности и защиты данных Huawei. — Хотим пригласить все заинтересованные стороны, в том числе клиентов, органы контроля, организации по стандартизации, поставщиков технологий и тестирующие организации, для обсуждения вопросов внедрения основных принципов кибербезопасности и сотрудничества в этой сфере. Вместе мы будем совершенствовать безопасность продуктов во всей отрасли».

На данный момент в отрасли до сих пор не сформирован единый подход, основанный на стандартах, в частности в сфере управления, технических возможностей, сертификации и сотрудничества.

«Риски в сфере кибербезопасности являются общей ответственностью всех игроков отрасли, — отметил Кен Ху. — Правительства, организации по стандартизации и поставщики технологий должны сотрудничать, чтобы сформировать единое понимание вызовов отрасли кибербезопасности. Нам необходимо поставить общие цели международного уровня, согласовать обязательства и объединить усилия для создания надежной цифровой среды, отвечающей вызовам настоящего и будущего». ***(Huawei открыла в Китае свой крупнейший Международный центр кибербезопасности // Компьютерное Обозрение (https://ko.com.ua/huawei_otkryla_v_kitae_svoj_krupnejshij_mezhdunarodnyj_centr_kiberbezopasnosti_137665). 11.06.2021).***

***

**«10 июня 2021 года, почти через год после выпуска своего первого проекта, Постоянный комитет Всекитайского собрания народных представителей принял Закон о безопасности данных («DSL») после третьего чтения.** DSL вступит в силу 1 сентября 2021 года, и у организаций останется менее трех месяцев на то, чтобы ознакомиться и подготовиться к одному из наиболее важных положений закона КНР в области защиты данных. Первый и второй проекты DSL были выпущены высшим законодательным органом КНР 28 июня 2020 года и 29 апреля 2021 года соответственно, и вы можете найти основные

выводы из первого проекта и основные изменения, внесенные вторым проектом, в наших предыдущих информационных бюллетенях (доступны здесь и здесь).

Каковы основные изменения окончательного варианта DSL по сравнению со вторым проектом?

Многих может утешить то, что версия пометок против второго проекта менее красочна, чем можно было бы ожидать: поправки не являются радикальными. Тем не менее, следует отметить следующие ключевые изменения:

*Новая концепция «Национальных основных данных»*

Согласно второму проекту DSL, центральному правительству поручено создать систему категоризации и классификации данных на национальном уровне, основанную на уровне важности данных для национальной безопасности и общественных интересов, а также на уровне воздействия любой утечки данных, фальсификации, повреждение или незаконное приобретение могут иметь отношение к национальной безопасности, общественным интересам или законным правам и интересам граждан или организаций. На региональном и отраслевом уровне регулирующим органам поручено выпускать специальные каталоги для определения объема «важных данных» в их соответствующих регионах или секторах на основе системы категоризации и классификации данных на национальном уровне. Такая центрально-местная / секторная структура системы категоризации данных остается неизменной в окончательном варианте DSL.

В окончательный DSL было добавлено понятие «основных национальных данных», которые относятся к данным, касающимся национальной безопасности, жизненного пути национальной экономики, средств к существованию людей и основных общественных интересов. В статье 21 предусматривается, что в отношении таких национальных основных данных должна применяться «более строгая система регулирования». Однако в DSL не уточняется, какой должна быть такая строгая регулирующая система, за исключением того, что в отношении штрафов орган может наложить штраф до 10 миллионов юаней в дополнение к другим штрафам за нарушение требований, касающихся национального ядра. данные. Ожидается, что дальнейшие разъяснения и правила, в частности, в отношении параметров «национальных основных данных» и соответствующей «строгой системы регулирования» будут выпущены в последующих правилах реализации.

*Обработка запросов данных от иностранных судебных или правоохранительных органов*

Некоторые изменения были внесены в положение, касающееся обработки запросов данных иностранными судебными или правоохранительными органами. Согласно первому проекту, если иностранный судебный или правоохранительный орган запрашивает доступ к данным, хранящимся в Китае, такие данные не должны предоставляться, если (i) не было получено разрешение от компетентного государственного органа, или (ii) соответствующий международный договор применяется. Во втором проекте вводилась оговорка о штрафных санкциях за нарушение этого требования, которая включала выдачу приказов об исправлениях, предупреждений и штраф в размере до 1 миллиона юаней для организации и до 200

000 юаней для ответственного лица и других непосредственно ответственных лиц. персонал.

В соответствии с окончательной версией DSL требования и соответствующие штрафы были ужесточены, в частности:

Утверждение требуется для всех видов предоставления данных: текущая редакция DSL предполагает, что одобрение компетентного государственного органа распространяется на все виды предоставления данных иностранным судебным или правоохранительным органам, включая те, которые охватываются международными договорами или соглашениями, заключенными Китаем. участвовал. Компетентный орган должен обрабатывать запрос данных в соответствии с такими договорами или соглашениями или в соответствии с принципом равенства и взаимной выгоды. Непонятно, как власти будут обрабатывать такие запросы на практике.

Более строгие штрафы: окончательный DSL предусматривает дополнительные штрафы за нарушения, которые приводят к серьезным последствиям, включая штраф до 5 миллионов юаней и штраф в размере менее 500 000 юаней для соответствующего ответственного персонала.

Вышеупомянутые требования в рамках DSL могут потенциально поставить MNC в неудобное положение: выполнение запроса на доступ к данным иностранного органа приведет к нарушению законодательства КНР, а несоблюдение запроса данных приведет к нарушению соответствующих иностранных законов или постановления суда.

*Обязательства компетентного органа в отношении конфиденциальности*

Государственные органы связаны DSL так же, как и частные стороны в соответствии с DSL. Кроме того, окончательный DSL конкретно включает дополнительные обстоятельства, когда компетентные органы обязаны соблюдать конфиденциальность. Сюда входят обстоятельства, когда отдельные лица и организации подают жалобу на нарушение DSL и, в более общем плане, личную информацию, коммерческую тайну, конфиденциальную деловую информацию и другие данные, ставшие известными во время выполнения своих обязанностей. Эти дополнительные обязательства помогут защитить интересы людей во время административных правоприменительных действий и связанных с ними процедур.

*Учет потребностей пожилых людей и инвалидов*

В окончательном варианте DSL добавлен новый и интересный пункт: при разработке и улучшении «интеллектуальных / интеллектуальных общественных услуг» необходимо полностью учитывать потребности пожилых людей и инвалидов, чтобы не создавать препятствий в их повседневной жизни. Похоже, что это первый случай, когда в нормативных актах КНР о защите данных прямо указываются потребности пожилых людей и инвалидов. Это важно в свете иерархии DSL, который является законодательным актом высокого уровня, обеспечивающим политику и руководство.

*Отношения с PIPL и CSL*

Как указано в наших информационных бюллетенях, DSL вместе с PIPL (который, как ожидается, будет выпущен в этом году) представляют собой два наиболее важных и долгожданных закона в области защиты данных в 2021 году,

почти через 4 года после вступления в силу PRC. Закон о кибербезопасности («CSL») в 2017 году. CSL, DSL и PIPL будут представлять собой три столпа китайской законодательной системы защиты данных и вместе образуют всеобъемлющую основу, регулирующую вопросы обработки данных и кибербезопасности.

CSL – это первое всеобъемлющее законодательство, формирующее основу защиты данных с точки зрения кибербезопасности. Он предусматривает обязательства по кибербезопасности для «сетевых операторов» и «операторов критически важной информационной инфраструктуры» («CIIO») в Китае.

Хотя CSL затрагивает вопросы безопасности данных, он остается общим и не фокусируется на структуре управления безопасностью данных. В ответ DSL теперь применяется для дальнейшего повышения безопасности данных за счет создания фундаментальной и категоризированной системы безопасности данных, применяемой потенциально ко всем действиям по обработке данных, независимо от того, являются ли они онлайн или офлайн.

В отличие от требований CSL и DSL, ориентированных на безопасность, PIPL фокусируется на защите личной информации и защите прав субъектов личной информации. DSL, вероятно, также будет применяться к личной информации, учитывая, что в статье 53 окончательной версии DSL говорится, что обработка личной информации «также» должна соответствовать другим законам и постановлениям. Это говорит о том, что, с одной стороны, обработка личной информации также подпадает под действие DSL, а с другой стороны, более конкретные правила и положения, регулирующие личную информацию, будут изложены отдельно в рамках еще не доработанной PIPL.

*Наблюдения*

Перчатки сняты. Компании, ведущие бизнес в Китае, должны предпринять активные и незамедлительные действия – если еще не были – для оценки того, применяется ли DSL к их деятельности по обработке данных внутри и за пределами Китая, и каким образом, и какие меры по обеспечению безопасности данных им следует принять в дальнейшем, прежде чем они станут эффективными DSL 1 сентября 2021 года. Ниже мы приводим краткий контрольный список, который компании могут использовать в качестве первоначальной оценки соответствия в течение короткого переходного периода:

Вы классифицировали данные, которые обрабатываете? Хотя окончательные каталоги все еще ожидаются, компании могут начать рассматривать, будут ли какие-либо данные, которые вы обрабатываете, рассматривать как «основные национальные данные», «важные данные» и / или «личную информацию»?

Если обрабатываемые вами данные попадают в эти строго регулируемые категории данных, ввели ли вы соответствующие меры и процедуры защиты в соответствии с DSL и другими применимыми отраслевыми и отраслевыми правилами и инструкциями? Например, проводятся ли у вас периодические оценки рисков при обработке «важных данных»?

Приняли ли вы меры для минимизации безопасности и рисков обработки данных, а также планы действий в чрезвычайных ситуациях для реагирования на инциденты с данными?

Выявили ли вы какую-либо обработку данных, которая может подлежать оценке национальной безопасности?

Вы создали систему управления безопасностью данных в своей компании? Например, проводили ли вы соответствующее обучение сотрудников, следовали ли вы схеме многоуровневой защиты для оценки вашей сетевой системы, назначили ли ответственное лицо за безопасность данных и т.д.?

Вы экспортируете данные за пределы Китая? Будьте готовы к более подробной информации о требованиях к трансграничной передаче данных, имея четкое представление о потоках данных в вашей компании.

Приняли ли вы меры и механизмы для ответа на запросы властей о доступе к имеющимся у вас данным?

Тем не менее, нерешенные вопросы остаются, и хотелось бы получить дальнейшие разъяснения, например, незавершенные классификации данных и каталоги «важных данных», каковы строгие требования, применимые к национальным основным данным, и отсутствие требований, касающихся экспорта «важных данных».», в частности для не-СПО, и это лишь некоторые из них. Стоит отметить, что «Положения об управлении безопасностью данных» и «Положения о защите безопасности СПО» были включены в законодательную повестку дня Государственного совета на 2021 год. Следовательно, компании должны продолжать контролировать нормативную разработку правил реализации после обнародования DSL». ***(Clarice Yue, Michelle Chan, Sharon Zhang, Tiantian Ke. Are you ready? PRC Data Security Law was Passed and will Come into Effect on 1 September 2021! // Bird & Bird (https://www.twobirds.com/en/news/articles/2021/china/prc-data-security-law-was-passed-and-will-come-into-effect-on-1-september-2021). 18.06.2021).***

***

## *Російська Федерація та країни ЄАЕС*

**«Дмитрий Песков сообщил, что Россия разрабатывает собственные стандарты обеспечения национальной кибербезопасности, а конечной целью является формирование информационного суверенитета.** При этом спецпредставитель президента России добавил, что наша страна зачастую сама становится объектом целевых кибератак, тщательно подготовленных зарубежными злоумышленниками. Песков напомнил, что власти занялись вопросом кибербезопасности уже несколько лет назад, однако для ощутимых результатов в этой области стране «понадобится не один год, даже не два и не пять». «Сегодня для России актуально создание собственных технологических стандартов, которые смогут вместе обеспечить кибербезопасность страны», — передаёт «РИА Новости» слова Дмитрия Пескова. При этом договориться о международных стандартах кибербезопасности в настоящий момент практически невозможно, отметил Песков. Эту ситуацию, по мнению спецпредставителя Путина, можно сравнить с криптовалютами». ***(Екатерина Быстрова. Песков обещает создание***

***собственных стандартов кибербезопасности в России // ООО «АМ-МЕДИА» (https://www.anti-malware.ru/news/2021-06-21-111332/36183). 21.06.2021).***

***

**«Ростелеком-Солар» сможет инициировать блокировку фишинговых сайтов в нескольких доменных зонах.** Такое право компания получила, заключив соглашения о защите интернет-пространства от нарушений с тремя российскими организациями, администрирующими домены. В частности, «Ростелеком-Солар» будет сотрудничать с АНО «Координационный центр национального домена сети интернет» (администрирует доменные зоны RU и.РФ), Фондом содействия развитию технологий и инфраструктуры интернета FAITID (администрирует домены. MOSCOW и.МОСКВА и 71 домен второго уровня) и АНО «РосНИИРОС» (администрирует домен верхнего уровня.SU).

Практика взаимодействия администраторов доменных зон с организациями, компетентными в определении нарушений в сети, существует в России уже более 10 лет. Обнаружив сайты, которые используются злоумышленниками для незаконной деятельности, такие организации сообщают об этом непосредственно регистраторам доменных имен и инициируют блокировку подозрительного ресурса. На данный момент партнерами Координационного центра являются 11 частных ИБ-компаний и государственных организаций, а FAITID и «РосНИИРОС» — 5.

«Из года в год мы видим кратный рост фишинговых атак, а в преддверии праздников и массовых отпусков или на фоне громких новостей количество поддельных интернет-сайтов с актуальной тематикой увеличивается на 30-40%. Статусы компетентной организации для ключевых российских доменных зон позволят нам занять более активную позицию в борьбе с фишингом и расширить наши возможности по реагированию на киберинциденты», — отметил директор центра противодействия кибератакам Solar JSOC компании «Ростелеком-Солар» Владимир Дрюков.

Данные о фишинговых ресурсах и ресурсах, распространяющих вредоносное программное обеспечение «Ростелеком-Солар» собирает из разных источников: статистика центра противодействия кибератакам Solar JSOC, анализ поисковой выдачи в интернете, а также мониторинг даркнета. Актуальная информация оперативно передается регистраторам доменных имен и администраторам доменных зон, что позволяет своевременно заблокировать доступ к сайту, который используется в противоправных целях. В среднем блокировка незаконного ресурса в вышеуказанных доменных зонах происходит в течение 1-2 дней». ***(Дмитрий Степанов. «Ростелеком-Солар» получил право инициировать блокировку фишинговых сайтов в Рунете // CNews (https://www.cnews.ru/news/line/2021-06-15_rostelekomsolar_poluchil). 15.06.2021).***

***

**«Заместитель лидера австралийских зеленых сенатор Ник МакКим сообщил Сенату, что его партия хочет отозвать находящийся на рассмотрении Закон о безопасности в Интернете, попросив изменить его проект, чтобы учесть ряд проблем, которые были подняты, но не решены в ходе коротких консультаций по законопроекту и период проверки.**

Среди прочего, Закон о безопасности в Интернете 2021 расширяет функцию кибер-удаления, выполняемую Уполномоченным по электронной безопасности, на взрослых, давая право отправлять уведомления об удалении непосредственно службам, на которых размещен контент, и конечным пользователям, ответственным за оскорбительный контент.

Тем временем Закон о безопасности в Интернете (переходные положения и последующие поправки) 2021 года отменяет Закон об усилении безопасности в Интернете 2015 года после вступления в силу нового Закона о безопасности в Интернете.

МакКим, как и многие другие, заявил, что правительство «проталкивает эти законопроекты через этот парламент без надлежащего рассмотрения и без надлежащей проверки».

Законопроект был внесен в парламент 24 февраля, через восемь рабочих дней после закрытия консультаций по законопроекту и до того, как были опубликованы 400 представлений для консультаций. Он был передан комитету Сената 25 февраля, и после проведения одного публичного слушания комитет, изучивший его содержание, представил свой отчет.

Правительство, добавил МакКим, затем стремилось к тому, чтобы законопроекты «быстро и незаметно» были приняты, и двинулось к освобождению законопроектов от обычных требований, которые регулируют, насколько быстро законопроекты могут быть вынесены на обсуждение в Сенате.

«И в качестве примера неприличной поспешности, с которой действовало правительство, эти законопроекты были настолько поспешными, что правительству необходимо использовать поправки для исправления опечаток в первоначальном законопроекте», – сказал он, обращаясь к Сенату в среду.

«Таким образом, эти законопроекты, которые предназначены для защиты людей от кибер-хулиганов, от кибер-злоупотреблений, от несанкционированного обмена интимными изображениями, а также от насильственных и экстремистских материалов – похвальные цели – проходят через это место».

Опечатка, которую упомянул МакКим, была неправильным написанием слова «запугивание».

В первоначальном законопроекте не было механизма подачи жалоб; с тех пор это было несколько исправлено, и уполномоченному по электронной безопасности была дана директива встать.

«В некотором смысле, парламент просят подписать бланк чека в отношении создания этого процесса. Потому что у нас нет возможности, когда мы стоим здесь и обсуждаем этот законопроект сегодня, знать, какой процесс будет выполнять Комиссар по электронной безопасности. установить ", – сказал он.

Он также сказал, что только потому, что действующему уполномоченному можно доверять, чтобы не злоупотреблять своими предстоящими широкими полномочиями, ее преемник может вести себя иначе.

«Парламент должен быть обязан удостовериться, что мы принимаем законы, имея в виду не только одного конкретного человека, занимающего одну конкретную должность, но и четко фокусируясь на необходимости гарантировать, что защита будет существовать за пределами полномочий любого одного человека. в любой конкретной позиции», – сказал он.

Дело не только в поспешном характере законопроектов, с которыми зеленые не согласились, поскольку они также выразили озабоченность по поводу предвзятости, которая может возникнуть из-за алгоритмов, которые были созданы для решения требований законопроекта.

«Законопроекты также неизбежно приведут к тому, что онлайн-платформы будут прибегать к автоматизированным процессам, основанным на алгоритмах и искусственном интеллекте, для выявления и удаления контента, который может повлечь за собой штрафы», – сказал он.

«Использование ИИ и алгоритмов в аналогичных обстоятельствах в таких странах, как США, было чрезвычайно спорным, если не сказать больше, и мы обеспокоены тем, что использование этих технологий может привести к непропорциональным результатам, таким как общие запреты, даже если это не так. намерение комиссара».

МакКим сказал, что использование алгоритмов и искусственного интеллекта также рискует внести расовые предубеждения в регулирование экосистемы онлайн-контента Австралии.

«Мы знаем, что это риск, потому что именно это и произошло в США в соответствии с аналогичными противоречивыми законами», – сказал он.

По его словам, с дискриминацией столкнутся и работники индустрии для взрослых.

«Мы обеспокоены непредвиденными последствиями, которые могут нанести вред как секс-работникам и взрослому бизнесу, так и более широкому сообществу», – сказал он. «Согласно законопроектам, как утверждает Scarlet Alliance, секс-работники станут более уязвимыми, поскольку они потенциально потеряют доступ к инструментам и стратегиям обеспечения безопасности доходов и жизненно важным связям со сверстниками. Мы также обеспокоены тем, что законопроекты не смогли обеспечить максимальную безопасность. и средства защиты конфиденциальности, которые они могли бы сделать.

«Зеленые абсолютно одобряют заявленные цели этих законопроектов по обеспечению безопасности женщин-детей и широкой австралийской общины в онлайн-среде… но мы должны убедиться, что мы не защищаем один набор прав, попирая другие права».

Он сказал, что законопроекты, столь важные и нацеленные на решение столь сложных проблем, должны пройти всестороннюю и надлежащую проверку.

«И это то, что, к сожалению, правительство пытается отрицать». ***(Asha Barbaschow. AI bias and discrimination aplenty: Australian Greens want Online Safety Bill repealed // ZDNet (https://www.zdnet.com/article/ai-bias-and-***

***discrimination-aplenty-australian-greens-want-online-safety-bill-repealed/). 16.06.2021).***

***

**«Австралийское управление сигналов опубликовало в четверг отчет о состоянии кибербезопасности Содружества в 2020 году, одним из ярких моментов которого стало использование сканирования Австралийским центром кибербезопасности (ACSC).**

В рамках своих программ улучшения кибергигиены (CHIP) ACSC смогла выявлять уязвимые, доступные в Интернете системы MobileIron в Содружестве, штатах и территориях, а также в местных органах власти.

«ACSC уведомил все государственные организации, эксплуатирующие уязвимые устройства, о деталях устройства, критической уязвимости и срочной необходимости исправления или иного снижения риска», – говорится в отчете.

«Эта своевременная и полезная информация от ACSC позволила некоторым правительственным организациям предотвратить использование их устройств MobileIron злоумышленником, в одном случае за несколько часов».

В отчете говорится, что уязвимости MobileIron и Citrix 2020 года были быстро устранены до того, как начали появляться попытки эксплуатации.

«Отчет показал, что злоумышленники пытались использовать эти уязвимости в течение нескольких дней после публичного обнародования кодов подтверждения концепции», – говорится в сообщении.

«Организации, которые не могут своевременно обновлять свои сервисы, подключенные к Интернету, особенно устаревшие VPN и веб-сайты, должны улучшить свои возможности исправления. Принятие облачных подходов" программное обеспечение как услуга «или» платформа как услуга "к выходу в Интернет услуги могут помочь».

В другом месте в отчете говорится, что, хотя в абсолютном выражении киберпозиционирование субъектов Содружества улучшается, сдвиг в 2020 году был ледяным.

Например, в отчете говорится, что организации улучшают защиту приложений, но только 12% организаций стали лучше. Точно так же 10,5% осуществляли контроль приложений должным образом, а еще 9,5% организаций могли сказать, что они правильно ограничивали права администратора.

Вина за медленные темпы была возложена на организации, продолжающие использовать устаревшие и неподдерживаемые операционные системы и приложения, не использующие облачные сервисы, организации, не имеющие быстрых или гибких стратегий модернизации, нехватку кибер-навыков и организации, продолжающие «неправильно понимать, неправильно интерпретировать и непоследовательно «Самая важная восьмерка.

В ответе правительства, представленном в среду, правительство рассматривает возможность сделать Essential Eight жизненно важным для своих предприятий.

Ограничение приверженности только первой четверкой из восьми основных показало, что 11% организаций сообщили о самом низком уровне соответствия, за

которыми следуют 55% на втором этапе четырехступенчатой системы, 33% на третьем уровне и только 1% полностью соответствует требованиям.

Политика с самым низким уровнем зрелости заключалась в «защите информации от киберугроз».

Положительным моментом является то, что CHIP теперь может отслеживать «показатели кибергигиены» в 71 300 активных государственных доменах Содружества, что на 54 300 доменов больше, чем в феврале 2020 года, и охватывает сайты 187 организаций.

В 2020 году CHIP получили возможность сканировать зашифрованную электронную почту; использовались ли на государственных сайтах новейшее программное обеспечение, отображались ли веб-сайты по умолчанию или использовались ли сертификаты с истекшим сроком действия; сканирование на наличие критических уязвимостей; и консультирование государственных органов на всех уровнях по услугам, которые они открывают для более широкого Интернета.

В течение года ACSC создала систему защитных доменных имен, которая блокирует домены, связанные с вредоносными программами, программами-вымогателями, фишинговыми атаками и другим вредоносным контентом.

«В рамках пилотного проекта ACSC обработал около 2 миллиардов запросов от восьми организаций Содружества в период с апреля по декабрь 2020 года и заблокировал 4683 уникальных вредоносных киберугрозы, предотвратив более 150 000 угроз», – говорится в отчете.

«В 2021–2022 годах эта возможность будет предложена всем субъектам Содружества».

В отчете говорится, что примерно четверть организаций сейчас используют DMARC для предотвращения спуфинга электронной почты.

В течение года ACSC заявила, что отреагировала на 434 киберинцидента, из которых 46% были зарегистрированы самостоятельно, а остальные были обнаружены с помощью расследований ACSC, отчетов международных партнеров и третьих сторон, а также анализа различных секретных и открытых источников материал»…». ***(Chris Duckett. ACSC scanning is allowing Commonwealth entities to avoid being hacked // ZDNet (https://www.zdnet.com/article/acsc-scanning-is-allowing-commonwealth-entities-to-avoid-being-hacked/). 10.06.2021).***

***

**«Недавно назначенный министр внутренних дел Карен Эндрюс выделила кибербезопасность в качестве приоритета в своем портфеле, используя реформы критической инфраструктуры Австралии в качестве примера того, как правительство работает над защитой нации.**

«Я поставил кибернетику на первое место в своем портфолио», – сказал Эндрюс, выступая в четверг на конференции CEDA State of the Nation 2021.

Реформы посредством законопроекта о внесении поправок в законодательство о безопасности (критическая инфраструктура) 2020 года позволят, среди прочего, правительству оказывать «помощь» организациям в ответ на серьезные кибератаки на австралийские системы. Технологические гиганты,

работающие в Австралии, такие как Amazon Web Services, Cisco, Microsoft и Salesforce, не согласны с этими полномочиями «в крайнем случае».

«Закон о критической инфраструктуре особенно важен для нас, и я думаю, что то, что он демонстрирует, – это восприятие людьми того, что является критически важной инфраструктурой, которая выходит за рамки физических кирпичей и строительного раствора, и имеет решающее значение для нас», – сказал Эндрюс.

Законопроект объединяет такие отрасли, как связь, финансовые услуги, хранение и обработка данных, высшее образование и исследования, энергетика, продукты питания и бакалея, здравоохранение и медицина, космические технологии, транспорт, водоснабжение и канализацию, к определению критически важной инфраструктуры.

«Мы знаем, что существует растущая угроза кибератак здесь, в Австралии, программ-вымогателей, это серьезные проблемы для нас. Также важно, чтобы мы осознавали, что многие компании, которые либо подверглись атакам программ-вымогателей, либо, вероятно, будут ", – продолжил Эндрюс, – подвергнуться атаке с использованием программ-вымогателей не обязательно будет немедленно предоставлять эту информацию.

@Если у нас нет информации, поступающей в Австралийское управление связи, которая позволяет им прийти и обеспечить определенный уровень поддержки, это означает, что мы не можем помочь в попытке восстановить некоторые из подключений, которые там, чтобы попытаться помочь с восстановлением данных. Это также означает, что мы не получаем необходимой информации, которая приведет к созданию более кибербезопасной среды для нас здесь, в Австралии».

Эндрюс сказал, что закон необходимо «в срочном порядке доработать»…

Рядом с Эндрюсом выступила Мишель Прайс, генеральный директор AustCyber, организации, отвечающей за развитие местной экосистемы кибербезопасности. Она рекламировала этот закон как «один кусок очень большого лоскутного одеяла вещей», который необходимо предпринять.

«Люди радуются принятию этого закона, главным образом потому, что он уравнивает правила игры во всех отраслях», – сказала она.

Однако для Прайса важно, чтобы просвещение относительно цели и последствий законопроекта должно было произойти.

«Мы должны убедиться, что это образование распространяется, именно здесь в него входит цепочка создания стоимости, те надежные сети обмена информацией, которые возникают органически, а также организованно, чтобы убедиться, что все знают об этом законодательстве» она добавила.

«Я думаю, что правительство проделало хорошую работу по извлечению некоторых уроков из законодательства о шифровании и провело обширные консультации по этому законодательству, несмотря на сравнительно короткий период времени, который он прошел, по сравнению с другими областями, такими как телекоммуникации. Реформы безопасности сектора и схема уведомляемых утечек данных… [которые] заняли гораздо больше времени, чем поправки к критически важной инфраструктуре».

Сенат на этой неделе принял два законопроекта, по которым также не было особо продолжительных периодов консультаций.

Билл Интернет Безопасности 2021 развевались через ночь на среду с поправками. Среди прочего, новый закон расширяет функцию удаления кибернетической информации Уполномоченного по электронной безопасности на взрослых, давая право отправлять уведомления об удалении непосредственно службам, на которых размещен контент, и конечным пользователям, ответственным за оскорбительный контент.

Законопроект был внесен в парламент 24 февраля, через восемь рабочих дней после закрытия консультаций по законопроекту и до того, как были опубликованы 400 представлений для консультаций. Он был передан комитету Сената 25 февраля, и после проведения одного публичного слушания комитет, изучивший его содержание, представил свой отчет.

Обсуждая законопроект на прошлой неделе, заместитель лидера австралийских зеленых сенатор Ник МакКим сказал, что правительство «[протаранило] эти законопроекты через этот парламент без надлежащего рассмотрения и без должной проверки».

Он не удовлетворил свою просьбу об отмене и переписывании законопроекта, и после получения королевского согласия eSafety будет уточнять спецификации того, как будет работать новая схема через шесть месяцев после этого.

На этой неделе также был принят закон о внесении поправок в законодательство о телекоммуникациях (международные производственные заказы) 2020 года.

Закон об IPO открывает для Австралии путь к обмену данными связи с другими странами. Это позволяет Австралии получить предлагаемое двустороннее соглашение с Соединенными Штатами, в первую очередь, по его Clarifying Действителен Overseas использования Закона данных (Закон CLOUD).

Законопроект был принят обеими палатами, в него были включены поправки из рекомендаций, внесенных Объединенным парламентским комитетом по разведке и безопасности (PJCIS) в прошлом месяце.

Федеральная оппозиция в понедельник внесла в парламент еще один законопроект, связанный с безопасностью, который, если он будет принят, потребует от организаций информировать Австралийский центр кибербезопасности (ACSC), прежде чем будет произведен платеж преступной организации в ответ на атаку программы-вымогателя.

Билл 2021 вымогателей Оплаты был введен в Палате представителей, помощник министра Теней для Cyber Security Тима Уоттс, который воспользовался возможностью, чтобы сказать текущую позицию правительства расскажет бизнес, чтобы защитить себя от «запирания двери в кибер-преступных группировки» был «не достаточно хорошо».

Отвечая на предложенный законопроект, Эндрюс сказала, что открыта для его изучения.

«С точки зрения правительства, мы действительно хотели бы, чтобы компании обращались, особенно к ACSC, в случае атаки программы-вымогателя или других угроз», – сказала она.

«[ACSC] имеет очень хорошие возможности для их поддержки, но во многих случаях они полагаются на то, что компании сообщают или связываются с ними напрямую.

«У меня уже было несколько дискуссий об обязательном сообщении об атаках программ-вымогателей, и я считаю, что на данном этапе существует ряд мнений по этому поводу – они очень неоднозначны в ответах – в ближайшие недели я хочу сделать следующее: изучить это гораздо более полно ".

Эндрю сказала, что она хочет, чтобы ACSC был вооружен возможностью поддерживать предприятия, которые подвергались атакам программ-вымогателей, но эта осведомленность также важна…». ***(Asha Barbaschow. Minister prioritises Critical Infrastructure Bill as two others pass through Parliament // ZDNet (https://www.zdnet.com/article/minister-prioritises-critical-infrastructure-bill-as-others-pass-through-parliament/). 25.06.2021).***

***

## *Інші країни*

**«После растущего числа кибератак, которые местные корпорации получили за последние пару лет, опыт в других юрисдикциях и рекомендации IAIS (Международная ассоциация страховых надзоров) чилийского регулирующего органа в области страхования (Comisión para el Mercado Financiero – CMF) недавно утвердил новое постановление, которое инструктирует страховые и перестраховочные компании в отношении операционных рисков и рисков кибербезопасности.**

В этом смысле, учитывая постоянную эволюцию рисков, связанных с киберпространством, и степень, в которой такая угроза может представлять чилийский страховой и финансовый сектор, норма устанавливает восемь фундаментальных элементов, установленных Основными элементами кибербезопасности G7. для финансового сектора и требует их соблюдения страховыми компаниями.

Соответственно, новая норма, вступающая в силу 30 сентября 2021 года, устанавливает обязательства страховщиков: i) информировать CMF об операционном происшествии в течение не более 30 минут с момента, когда компания узнала о его возникновении; ii) незамедлительно сообщать клиентам или пользователям, когда инцидент влияет на качество или непрерывность услуг Страховщиков, с необходимостью обновлять доступную информацию до тех пор, пока инцидент не будет преодолен; iii) информировать отрасль. Об инцидентах, связанных с киберпространством, необходимо будет сообщать остальной части отрасли, чтобы предотвратить потенциальные угрозы, обеспечить раннее обнаружение, реагирование и восстановление и, в конечном итоге, уменьшить распространение негативных воздействий в системе.

В целом, это следует рассматривать как шаг вперед в развитии продуктов киберрисков в Чили, поскольку местные компании не понаслышке знают о сложностях и проблемах, которые они создают». ***(María Jesús Pérez. New operational and cyber risks standards in Chile // DAC Beachcroft LLP (https://www.dacbeachcroft.com/en/articles/2021/june/new-operational-and-cyber-risks-standards-in-chile/). 28.06.2021).***

***

## Кібервійни та протидія зовнішній кібернетичній агресії

**«Оскільки Росія активізує кібербойові дії, а Китай «озброює» штучний інтелект, об'єднання зусиль у галузі кібербезпеки займатиме важливе місце в списку тем, які будуть обговорювати союзники НАТО на саміті наступного тижня.** Але 30 членам трансатлантичного альянсу потрібно рухатись швидко, якщо вони прагнуть компенсувати втрачені позиції в нову епоху кіберпротистояння…

НАТО пропонує створити новий центр технологічних інновацій, що об'єднає військову сферу для сприяння стартапам цифрової оборони. Деякі ініціативи можуть бути профінансовані окремо, для прикладу, фонд венчурного капіталу для інновацій.

Однак Захід дещо відстає у питанні цифрової оборони, це визнав і сам генеральний секретар НАТО Єнс Столтенберг.

«Десятиліттями союзники НАТО були лідерами у технологічній сфері, але це лідерство вже не таке очевидне останнім часом», – сказав він в інтерв'ю для Financial Times минулого тижня.

«Ми бачимо, що Китай особливо активно інвестує в нові технології, такі як штучний інтелект, автономні системи, великі обсяги даних. Пекін застосовує їх у нових передових системах зброї, безпілотниках, підводних човнах, літаках тощо», – додав Столтенберг.

Генсек НАТО не перший почав бити на сполох. Колишній виконавчий директор Google Ерік Шмідт, який нині очолює Комісію з питань національної безпеки США щодо штучного інтелекту, попереджав ще на початку цього року, що Пекін планує «підірвати» звичайні збройні сили шляхом переходу до нових технологій.

У звіті комісії, опублікованому в березні, висловлено занепокоєння відносно того, що Китай використовуватиме штучний інтелект для «розвідки, контрзаходів та скоординованих ударів».

Частина проблеми полягає в тому, що західні оборонні установи повільно розпізнавали потенціал інновацій за межами власної галузі.

«Протягом десятиліть у оборонному секторі відбулося багато технологічного розвитку – Інтернет, атомна енергія, GPS, все це було розроблено оборонною промисловістю, а потім передано цивільному сектору», – сказав Столтенберг.

«Зараз все йде навпаки. Саме цивільний сектор є провідним у розвитку штучного інтелекту, квантових обчислень та багатьох нових технологій», – додав Генсекретар НАТО.

Деякі члени НАТО випереджають інших у сфері «цифрового захисту». США та Франція опублікували військові стратегії ШІ, тоді як Велика Британія цього року оголосила, що планує створити «центр оборонного ШІ». Вперше британське розвідувальне відомство МІ6 обирає керівника своєї «технологічної лабораторії» з приватного сектору.

Створення нового центру НАТО, в якому технологічні компанії та члени збройних сил можуть експериментувати з новими ідеями, має переваги, на думку професора Фіони Мюррей.

Стартапи та інвестори не завжди встигають вирішити оборонні проблеми, коли рішення «важко перевірити, ринки роздроблені, а закупівлі йдуть повільно», каже Мюррей.

Спільна робота створила б більш широкий ринок нових технологій та підвищила б колективну безпеку, зазначає професор. За її словами, індивідуального вирішення цих питань кожною країною може бути «недостатньо».

США розпочали закликати союзників зважати на політичні наслідки використання нових технологій.

«Партнерство з питань штучного інтелекту в обороні» Пентагону, що включає 13 країн (серед них Канада, Данія, Естонія, Велика Британія, Франція та Норвегія), фактично вперше провело зустріч минулого року, щоб узгодити спільні військові стандарти щодо ШІ. Комісія закликала альянс до обміну розвідданими.

Експерт з військових технологій при Європейській раді з міжнародних відносин Ульріке Франке стверджує, що технологічний центр НАТО буде найбільш ефективним, якщо він надасть пріоритети системам, призначеним для сприяння спільним військовим операціям.

За її словами, альянс повинен розглянути такі сфери, як управління системами ШІ, що може дати членам єдину картину поля бою в різних регіонах, використовуючи аналіз даних для «фільтрування» інформації.

Франке вважає, що на «величезній арені», яка охоплює все, від безпілотників до квантових обчислень, існує спокуса «надмірного розпорошення уваги».

«Для НАТО є сенс більше зважати на нові технології. Питання в тому, на чому саме вони зосереджуються», – сказала Ульріке Франке…» ***(Анастасия Гурин. Нову епоху протистояння між країнами визначають кібервійни — FT // Дзеркало тижня. Україна (https://zn.ua/ukr/WORLD/novu-epokhu-protistojannja-mizh-krajinami-viznachajut-kibervijni-ft.html). 10.06.2021).***

***

**«Коммюнике, выпущенное по завершении саммита НАТО, призывает Китай соблюдать законы киберпространства и устанавливает новые стандарты, в соответствии с которыми члены альянса будут рассматривать кибератаки.**

Новый стандарт ссылается на статью 5 Североатлантического договора 1949 года, поскольку в ней говорится, что нападение на одного члена НАТО считается актом насилия против всех членов и заслуживает возмездия.

В новом коммюнике альянса из 30 стран, выпущенном после его саммита в понедельник, говорится, что статья 5 может применяться к кибератакам.

В коммюнике говорится:

Мы подтверждаем, что решение о том, когда кибератака приведет к применению статьи 5, будет приниматься Североатлантическим советом в индивидуальном порядке ".

Союзники признают, что воздействие значительных кумулятивных злонамеренных действий в киберпространстве при определенных обстоятельствах может рассматриваться как вооруженное нападение.

НАТО заявила, что готова «всегда использовать весь спектр возможностей для активного сдерживания, защиты и противодействия всему спектру киберугроз, в том числе проводимых в рамках гибридных кампаний, в соответствии с международным правом».

В документе и Россия, и Китай рассматриваются как угрозы. Россия получила 63 упоминания и отмечена как «агрессивная». Китай упоминается десять раз, и его поведение описывается как «напористое» и «создающее системные проблемы». В документе содержится обещание привлечь Китай к защите интересов безопасности Североатлантического союза, в частности, касаясь кибератак, кампаний дезинформации и действий Китая в космической сфере.

Днем ранее G7 опубликовала коммюнике саммита Carbis Bay G7, в котором призвала Россию «выявлять, пресекать и привлекать к ответственности тех, кто в пределах ее границ проводит атаки программ-вымогателей, использует виртуальную валюту для отмывания выкупа и другие киберпреступления». В коммюнике G7 также содержится призыв Китая к нарушениям прав человека, в частности, в отношении Синьцзяна и уйгурского населения, а также нарушений свободы в Гонконге.

Директор Управления Центральной комиссии Китая по иностранным делам Ян Цзечи по телефону опроверг обвинения в нарушении прав человека госсекретарю США Энтони Блинкену, заявив, что «некоторые антикитайские силы пытаются одну за другой вызвать зловещие волны, чтобы очернить Китай».

Китай – не единственная страна, недовольная некоторыми деталями многостороннего саммита в эти выходные. Страна-гость Индия отказалась подписать первую копию Заявления об открытых обществах «Большой семерки» и «Страны-гости: 2021», поскольку в нем отключение интернета осуждается как нарушение свободы выражения мнений. Позже Индия приняла пересмотренную версию, осуждающую только «отключение интернета по политическим мотивам».

В прошлом Индия отказала в интернет-услугах Джамму и Кашмиру, индийскому штату с мусульманским большинством, который был лишен полуавтономного статуса в 2019 году по соображениям безопасности. Страна также приказала закрыть фермы во время протестов фермеров, сославшись на вероятность насилия на таких мероприятиях. Оба отключения были широко интерпретированы как политически мотивированные попытки заглушить голоса

несогласных». ***(Laura Dobberstein. NATO summit communiqué compares repeat cyberattacks to armed attacks – and stops short of saying 'one-in, all-in' rule will always apply // The Register (https://www.theregister.com/2021/06/15/nato_final_communique_cyber_policy/). 15.06.2021).***

***

**«Британия заявила ООН, что международное киберправо должно допускать цифровое наказание с нулевым уведомлением, направленное на страны, атакующие чужую инфраструктуру.**

В заявлении, сделанном британскими дипломатами Группе правительственных экспертов ООН по развитию ответственного поведения государства в контексте международной безопасности (ГПЭ ООН), содержится призыв к международному праву разрешить ответные меры за кибератаки без уведомления.

«Соединенное Королевство не считает, что государства, принимающие контрмеры, юридически обязаны направлять предварительное уведомление (в том числе призывать государство, ответственное за международно-противоправное деяние, соблюдать нормы международного права) при любых обстоятельствах», – говорится в заявлении Великобритании ГПЭ ООН. сделано в преддверии встречи глав правительств Большой семерки в Корнуолле на этой неделе.

Это заявление знаменует собой разрыв с осторожной британской политикой, начатой всего два года назад, когда тогдашний министр иностранных дел Джереми Хант предупредил, чтобы «кибервмешательство» не стало «обычным явлением». Однако это соответствует слегка агрессивной риторике, примененной Министерством обороны в его Комплексном обзоре ранее в этом году.

Источники в правительстве и политике ранее сообщали The Register, что политика Великобритании направлена на достижение международного консенсуса в отношении кибернормативов, что упрощает противостояние России, Китаю, Ирану и подобным кибер-мошенникам.

Еще в 2019 году Хант сказал, что Великобритания должна быть «более решительной в отношении того, что мы считаем неприемлемым поведением и последствиями любого нарушения международного права», при этом смягчая это предупреждениями о нормализации международного взлома, но при нынешнем министре иностранных дел Доминике Раабе это кажется Представители британской политики меньше обеспокоены разжиганием международной напряженности.

«Любое решение прибегнуть к контрмерам без предварительного уведомления должно быть необходимым и соразмерным цели побуждения к соблюдению в данных обстоятельствах», – добавлено в документе GGE Великобритании, в знак признательности тем, кто хочет, чтобы всемирная паутина оставалась безопасным (безопасным) местом. вести дела и взаимодействовать с другими.

Поскольку западный мир колеблется от атак программ-вымогателей, исходящих в основном из России и стран, связанных с Россией, призыв к цифровым ответным действиям без предупреждения можно рассматривать как

усиление давления на эти страны. Британия также негласно хвасталась такими инициативами, как Национальные киберсилы, наступательное хакерское подразделение, якобы посвященное атакам онлайн-врагов правительства.

Поддержка увеличения использования оружия в киберпространстве со стороны видных британских деятелей была вялой: в прошлом году экс-глава NCSC Кьяран Мартин высказал мнение, что политики были «на удивление почтительными и, следовательно, беспрекословными», когда представили оружейные возможности NCF.

«Предварительное уведомление не может быть юридическим обязательством при ответе на скрытое кибер-вторжение с помощью контрмер или когда приходится прибегать к контрмерам, которые сами по себе зависят от скрытых кибер-возможностей». ***(Gareth Corfield. UK tells UN that nation-states should retaliate against cyber badness with no warning // The Register (https://www.theregister.com/2021/06/11/uk_ungge_cyber_norms_submission/). 11.06.2021).***

***

**«Высокопоставленные политики и официальные лица Польши подверглись «широкомасштабной» кибератаке, которая, по словам страны, исходила из России.**

«Наиболее важные польские официальные лица, министры и депутаты различных политических партий подверглись кибератаке», – говорится в заявлении Ярослава Качиньского, самого влиятельного политического деятеля Польши и председателя Комитета по делам национальной безопасности и обороны.

В ходе расследования польских и «союзных» спецслужб выяснилось, что «кибератака была осуществлена с территории Российской Федерации. Его масштабы и диапазон огромны», – сказал Качиньский.

По словам дипломата ЕС, осведомленного об инциденте, «оперативный и технический анализ, проведенный польскими национальными группами реагирования на инциденты кибербезопасности, подтвердил, что инфраструктура и методы работы, использованные во время кибератак, были такими же, как и у организаций, спонсируемых Россией».

«Пострадали более 30 парламентариев, представителей правительства и несколько журналистов», – добавил дипломат. «Атаки начались в сентябре 2020 года».

Польша сегодня призвала страны ЕС в Совете ЕС провести на уровне министров дебаты о том, как реагировать на нападения, сказал дипломат, добавив, что этот вопрос будет обсуждаться министрами иностранных дел в понедельник.

«В пятницу Польша передала странам-членам ЕС, Европейской комиссии и Совету документ с подробностями кибератак, совершенных в последние дни», – добавил дипломат.

В заявлении Качиньского говорится, что службы кибербезопасности находятся в процессе информирования политиков и официальных лиц, пострадавших в результате атаки». ***(LAURENS CERULUS. Polish politicians hit by***

***‘large-scale’ cyberattack, Russia blamed // Politico (https://www.politico.eu/article/polish-politics-hit-with-by-cyberattack/). 18.06.2021).***

***

**«Генеральный секретарь НАТО предупредил, что кибератаки могут привести к военному ответу со стороны ее союзников.**

Йенс Столтенберг сказал BBC Newsnight, что атака в киберпространстве «может быть столь же разрушительной и опасной», как вооруженное нападение, и «столь же серьезно, как любое другое нападение на союзника по НАТО».

Глава НАТО сказал, что в статье 5 договора организации говорится, что нападение на одного из ее союзников – это нападение на всех.

По словам Столтенберга, члены альянса, в который входят 30 европейских и североамериканских стран, могут отреагировать на кибератаки с воздуха, моря или земли». ***(Nato: Cyber attacks 'as serious as any other attacks' to allies // BBC (https://www.bbc.com/news/av/world-57478561). 15.06.2021).***

***

## Кіберзахист критичної інфраструктури

**«В апреле 2021 года Министерство энергетики (DOE) запустило 100-дневную инициативу по усилению защиты кибербезопасности в энергетическом секторе. Всего через месяц Управление транспортной безопасности (TSA), агентство, находящееся в ведении Министерства внутренней безопасности (DHS), выпустило Директиву по безопасности 2021-1 (Директива или Директива по безопасности), чтобы ввести – впервые – в обязательном порядке. требования к некоторым операторам трубопроводов в отношении кибербезопасности.** Директива о безопасности вступила в силу в день ее опубликования 28 мая 2021 года. Хотя Директива по безопасности была выпущена в окончательном виде, TSA принимает общественные комментарии к Директиве и указало, что может вносить поправки в Директиву на основе этих комментариев.

Директива о безопасности требует, чтобы владельцы и операторы инфраструктуры трубопроводов для «критических» опасных жидкостей и природного газа соблюдали определенные части инициативы Министерства энергетики, принятой в апреле 2021 года. Согласно определению Директивы, «критически важными» объектами трубопроводов являются те, которые ранее были определены TSA как критические в соответствии с Рекомендациями по реализации Закона о комиссии 9/11 от 2007 года и как указано в рекомендациях TSA по безопасности трубопроводов. Для этих владельцев и операторов Директива имеет три широких мандата.

*Отчетность об инцидентах в области кибербезопасности*

Во-первых, это требует, чтобы владельцы и операторы сообщали о случаях кибербезопасности в Агентство по кибербезопасности и безопасности инфраструктуры (CISA) DHS. В соответствии с этим требованием владельцы и

операторы должны сообщать «об инцидентах кибербезопасности» (как определено в Директиве) в CISA как можно скорее, но не позднее, чем через 12 часов после выявления такого инцидента. Если владельцы и операторы не могут собрать всю необходимую информацию в течение 12 часов, они должны «представить первоначальный отчет в указанные сроки и дополнить его по мере появления дополнительной информации». Сообщаемые инциденты кибербезопасности включают:

Несанкционированный доступ к системе информационных технологий (ИТ) или операционных технологий (ОТ);

Обнаружение вредоносного ПО в системе ИТ или ОТ;

Действия, приводящие к отказу в обслуживании любой ИТ– или ОТ-системы;

Физическая атака на сетевую инфраструктуру владельца или оператора; а также

Любой другой инцидент, который приводит к нарушению работы ИТ– или ОТ-систем или других аспектов трубопровода или иным образом может вызвать сбои в работе, которые отрицательно влияют на безопасную и эффективную транспортировку жидкостей и газов.

*Назначение координатора по кибербезопасности*

Во-вторых, Директива о безопасности требует, чтобы владельцы и операторы назначили координатора по кибербезопасности, который должен быть доступен для TSA и CISA 24 часа в сутки, семь дней в неделю, чтобы «координировать действия в области кибербезопасности и устранять любые возникающие инциденты». В рамках этой роли координатор будет нести ответственность за внутреннюю организацию практики кибербезопасности, взаимодействие с TSA и CISA, а также работу с соответствующими правоохранительными органами и агентствами по реагированию на чрезвычайные ситуации.

Оценка уязвимости должна быть завершена до 27 июня 2021 г.

Наконец, Директива о безопасности требует, чтобы владельцы и операторы проводили «оценку уязвимости» в течение 30 дней после принятия Директивы. Этот процесс требует, чтобы операторы сравнивали свои текущие практики с руководящими принципами TSA по обеспечению кибербезопасности трубопроводов для оценки рисков, выявления любых пробелов и разработки мер по исправлению положения, а также сроков реализации этих мер по исправлению положения. Операторы должны сообщать о выводах этой оценки в TSA и CISA…» ***(Catherine D. Little, Annie M. Cook, Mandi Moroz & Meg Heyse. Mandatory Homeland Security Cybersecurity Directive // Troutman Pepper Hamilton Sanders LLP (https://www.pipelaws.com/2021/06/mandatory-homeland-security-cybersecurity-directive/#page=1). 17.06.2021).***

***

**«Согласно исследованию центра противодействия кибератакам Solar JSOC компании «Ростелеком-Солар», каждая десятая российская организация из числа субъектов критической информационной инфраструктуры (КИИ) уже скомпрометирована различными семействами вредоносного ПО.** Помимо этого, часть уязвимостей, которые эксперты находят в объектах КИИ, хоть и были

опубликованы еще 10 лет назад, до сих пор не закрыты. Таким образом, совершить успешную атаку на большинство критически важных для страны инфраструктур могут даже хакеры с низкой квалификацией.

В декабре 2019 г. «Ростелеком» анонсировал запуск на своей инфраструктуре сети сенсоров и ловушек (honeypots) для раннего выявления атак. В ходе анализа данных с сенсоров команда Solar JSOC CERT отметила наибольшую активность четырех типов вредоносного ПО: Glupteba, PonyStealer, Trojan-Spy.Win32.Windigo и NjRAT. Основные цели Glupteba – кража пользовательских данных и добыча криптовалюты, при этом вредонос тщательно скрывает следы своего присутствия. PonyStealer – ботнет, известный с 2011 г. и предназначенный для похищения паролей учетных записей и другой чувствительной информации. Trojan-Spy.Win32.Windigo осуществляет рассылку спама, кражу конфиденциальных данных и кликфрод. NjRAT (он же Bladabindi) – троян 2012 г., используемый злоумышленниками для удаленного администрирования.

Это вирусное ПО, несмотря на свою несовременность, несет существенные риски для компаний. В случае если профессиональная группировка захочет развить свою атаку, ей достаточно приобрести в даркнете доступ к скомпрометированным узлам. Далее с помощью современных инструментов она сможет получить гораздо более глубокий доступ к инфраструктуре и повлиять на непрерывность бизнес-процессов, а также осуществить хищение конфиденциальной корпоративной информации или денежных средств.

Остаются актуальными и проблемы защиты периметра. В многих компаниях встречаются старые, но функциональные уязвимости. Причина этого в том, что процесс обновления ПО отсутствует в более чем 90% организаций, а среднее время установки обновлений составляет более 42 дней, отмечают эксперты Solar JSOC. Наиболее распространенные из уязвимостей: появившаяся в 2011 г. Heartbleed, EternalBlue (в 2017 г. она стала причиной распространения шифровальщика WannaCry) и BlueKeep, обнаруженная в 2019 г. Все они активно используются хакерами для реализации кибератак.

«Соблюдение кибергигиены – будь то устранение «дыр» на периметре организации или покрытие инфраструктуры средствами защиты – непростая, но критически важная задача. Ведь в текущей парадигме взаимодействия киберпреступного сообщества даже забытое старое ВПО может быть перекуплено профессиональной группировкой и использоваться в развитии сложной целенаправленной атаки», — отметил Владимир Дрюков, директор центра противодействия кибератакам Solar JSOC компании «Ростелеком-Солар».

Пандемия также значительно ослабила ИТ-периметры. За последний год более чем на 60% выросло число автоматизированных систем управления технологическими процессами (АСУ ТП), доступных из интернета. Это увеличивает риски промышленного шпионажа и кибертерроризма.

Кроме того, почти в два раза увеличилось количество хостов с уязвимым протоколом SMB. Это сетевой протокол для общего доступа к файлам, принтерам и другим сетевым ресурсам, который применяется практически в каждой организации. Такие уязвимости особенно опасны, так как позволяют хакерам

удаленно запускать произвольный код без прохождения аутентификации, заражая вредоносным ПО все компьютеры, подключенные к локальной сети.

Основной же проблемой во внутренних сетях является некорректное управление паролями. Крайне распространены слабые и словарные пароли, которые позволяют злоумышленнику проникнуть во внутреннюю сеть организации. Подбор пароля используют как хакеры-любители, так и профессиональные злоумышленники. Последних скомпрометированная учетная запись избавляет от необходимости преодолевать внешние средства защиты организации». ***(Дмитрий Степанов. Исследование: в России каждая десятая организация – субъект КИИ заражена вредоносным ПО // CNews (https://safe.cnews.ru/news/line/2021-06-02_issledovanie_v_rossii_kazhdaya). 02.06.2021).***

***

**«В первой половине 2021 года, в России было зафиксировано почти в 3 раза больше атак на объекты критической инфраструктуры, чем за весь за весь 2019 год. Об этом заявил Никита Кислицин, руководитель департамента сетевой безопасности Group-IB.**

К проблемам с обслуживанием ИТ-инфраструктуры организаций приводит недостаток ресурсов, устаревшее программное обеспечение и зачастую невыстроенный процесс патч-менеджмент (процесс закрытия уязвимостей, благодаря своевременным обновлениям программного обеспечения), а значит они являются потенциальной мишенью для киберпреступников, сообщили в Group-IB.

На текущий момент, по данным Group-IB Threat Intelligence & Attribution, суммарно 137 групп, из которых 122 киберкриминальных групп и 15 прогосударственных групп, нацелены на объекты критической инфраструктуры. Основная мотивация киберкриминальных групп по-прежнему финансовая, большую часть от их числа составляют сегодня «вымогатели», то есть хакеры, атакующие организации с целью выкупа за расшифровку данных. Целями проправительственных хакерских групп являются шпионаж, саботаж и диверсии. Group-IB приводит статистику: количество атак на объекты критической инфраструктуры в мире с 2019 года выросло в 12 раз (2019 vs H12021).

В первой половине 2021 года, в России было зафиксировано почти в 3 раза больше атак, чем за весь за весь 2019 год. За первые 6 месяцев 2021 года, 40% атак на объекты КИИ в России, были совершены киберкриминалом, 60% — прогосударственными атакующими.

В ходе мероприятия представители Group-IB представили собственные технологии для защиты от подобного рода атак. Компания официально сообщила, что выходит на рынок обеспечения кибербезопасности для промышленных сетей с новой разработкой Threat Hunting Framework Industrial. Это первая единая автономная платформа, создающая сквозную защиту всего предприятия, включая промышленные и ИТ-сети, а также рабочие места сотрудников.

Система автоматизировано коррелирует и группирует все сетевые события в инциденты для сокращения времени их обработки службами безопасности, инженерами и ИТ-специалистами. Именно таким образом ни одно событие, даже

на несколько секунд включенный в конечную станцию модем, не останется незамеченным «компьютерным зрением» THF Industrial: она «увидит» и проанализирует критичность этого события, помогая выстроить этапы реагирования на инцидент.

«Такие системы как Threat Hunting Framework Industrial должны работать на каждом производственном предприятии в стране, так как в ином случае они не защищены от остановки производства вследствие кибератаки», — заявил представитель Group-IB». ***(Владимир Бахур. Group-IB: количество атак на объекты критической инфраструктуры в мире выросло в 12 раз // CNews (https://safe.cnews.ru/news/line/2021-06-28_groupib_kolichestvo_atak_na). 28.06.2021).***

***

## Захист персональних даних

**«Исследователи обнаружили еще один массив конфиденциальных данных – головокружительную базу данных объемом 1,2 ТБ, содержащую учетные данные для входа, файлы cookie браузера, данные автозаполнения и платежную информацию, извлеченную вредоносным ПО, которую еще предстоит идентифицировать.**

В целом исследователи из NordLocker заявили в среду, что база данных содержит 26 миллионов учетных данных, 1,1 миллиона уникальных адресов электронной почты, более 2 миллиардов файлов cookie браузера и 6,6 миллиона файлов. В некоторых случаях жертвы сохраняли пароли в текстовых файлах, созданных с помощью приложения «Блокнот».

Тайник также включал более 1 миллиона изображений и более 650 000 файлов Word и.pdf. Кроме того, вредоносная программа сделала снимок экрана после того, как заразила компьютер, и сделала снимок с помощью веб-камеры устройства. Похищенные данные также поступали из приложений для обмена сообщениями, электронной почты, игр и обмена файлами. Данные были извлечены в период с 2018 по 2020 год с более чем 3 миллионов компьютеров.

*Быстро развивающийся рынок*

Это открытие произошло на фоне эпидемии нарушений безопасности, связанных с программами-вымогателями и другими типами вредоносных программ, поражающих крупные компании. В некоторых случаях, включая майскую атаку программ-вымогателей на Colonial Pipeline, хакеры сначала получали доступ, используя скомпрометированные учетные записи. Многие такие учетные данные доступны для продажи в Интернете.

Алон Гал, соучредитель и технический директор охранной фирмы Hudson Rock, сказал, что такие данные часто сначала собирает вредоносное ПО-кража, установленное злоумышленником, пытающимся украсть криптовалюту или совершить преступление аналогичного типа.

Злоумышленник «вероятно, затем попытается украсть криптовалюту, и как только он закончит с информацией, он будет продавать ее группам, специализирующимся на программах-вымогателях, взломе данных и корпоративном шпионаже», – сказал мне Гэл. «Эти кражи собирают пароли браузера, файлы cookie, файлы и многое другое и отправляют их на [командный сервер] злоумышленника».

Исследователи NordLocker заявили, что у злоумышленников нет недостатка в источниках для защиты такой информации.

«По правде говоря, каждый может заполучить нестандартное вредоносное ПО», – пишут исследователи. «Это дешево, легко настраивается, и его можно найти по всему Интернету. Реклама этих вирусов в даркнете раскрывает еще больше правды об этом рынке. Например, любой может получить собственное вредоносное ПО и даже уроки по использованию украденных данных всего за 100 долларов. А индивидуальный заказ действительно означает индивидуальный заказ – рекламодатели обещают, что они могут создать вирус для атаки практически на любое приложение, необходимое покупателю».

NordLocker не смог идентифицировать вредоносное ПО, использованное в этом случае. Гэл сказал, что с 2018 по 2019 год широко используемыми вредоносными программами были Azorult, а в последнее время – программа для кражи информации, известная как Raccoon. После заражения компьютер будет регулярно отправлять украденные данные на сервер управления и контроля, которым управляет злоумышленник.

В целом вредоносная программа собрала учетные данные почти 1 миллиона сайтов, включая Facebook, Twitter, Amazon и Gmail. Из 2 миллиардов извлеченных файлов cookie 22 процента оставались действительными на момент обнаружения. Файлы могут быть полезны для сведения воедино привычек и интересов жертв, и если файлы cookie используются для аутентификации, они предоставляют доступ к онлайн-аккаунтам человека. Здесь NordLocker приводит другие цифры.

Люди, которые хотят определить, были ли их данные захвачены вредоносным ПО, могут проверить службу уведомления о взломе Have I Been Pwned, которая только что загрузила список скомпрометированных учетных записей». ***(DAN GOODIN. Mystery malware steals 26M passwords from millions of PCs. Are you affected? // Condé Nast (https://arstechnica.com/gadgets/2021/06/nameless-malware-collects-1-2tb-of-sensitive-data-and-stashes-it-online/). 09.06.2021).***

***

**«Американское подразделение Volkswagen AG (VOWG_p.DE) заявило, что утечка данных у поставщика затронула более 3,3 миллиона клиентов и потенциальных покупателей в Северной Америке.**

Почти все пострадавшие были нынешними или потенциальными клиентами Audi, одного из люксовых брендов немецкого автопроизводителя.

Volkswagen Group of America заявила в пятницу, что неавторизованная третья сторона получила ограниченную личную информацию о клиентах и заинтересованных покупателях от поставщика, который его бренды Audi

Volkswagen и некоторые дилеры в США и Канаде использовали для цифровых продаж и маркетинга.

Информация собиралась для продаж и маркетинга в период с 2014 по 2019 год и находилась в электронном файле, который поставщик оставил незащищенным.

Компания сообщила регулирующим органам, что у подавляющего большинства клиентов есть только номера телефонов и адреса электронной почты, на которые потенциально может повлиять утечка данных. В некоторых случаях данные также включают информацию о приобретенном, арендованном или запрашиваемом автомобиле.

По заявлению VW, у 90 000 клиентов Audi и потенциальных покупателей были затронуты конфиденциальные данные, связанные с правом на покупку или аренду. VW заявила, что будет предлагать этим лицам бесплатные услуги по защите кредита.

Конфиденциальные данные состояли из номеров водительских прав в более чем 95% случаев. Небольшое количество записей включало дополнительные данные, такие как даты рождения, номера социального страхования и номера счетов.

Автопроизводитель не считает, что конфиденциальная информация задействована в Канаде.

Более 3,1 миллиона пострадавших проживают в Соединенных Штатах.

VW считает, что данные были получены в период с августа 2019 года по май этого года, когда автопроизводитель определил источник инцидента». ***(David Shepardson. VW says data breach at vendor impacted 3.3 million people in North America // Reuters (https://www.reuters.com/business/autos-transportation/vw-says-data-breach-vendor-impacted-33-million-people-north-america-2021-06-11/). 11.06.2021).***

***

**«Исследователи из Университета Маккуори обнаружили то, что они назвали серьезными проблемами с конфиденциальностью и непоследовательной политикой конфиденциальности в приложениях для здоровья.**

По оценкам исследователей, чуть более 99 000 приложений из 2,8 миллиона в Google Play и 1,96 миллиона в Apple App Store связаны со здоровьем и фитнесом. Они включают в себя управление состоянием здоровья и проверку симптомов, а также счетчики шагов и калорий и трекеры менструации.

Они исследовали 15 000 бесплатных приложений для здоровья в магазине Google Play и сравнили свои методы обеспечения конфиденциальности со случайной выборкой из более чем 8 000 приложений, не связанных со здоровьем. Они обнаружили, что, хотя эти приложения собирают меньше пользовательских данных, чем другие типы мобильных приложений, 88% могут получать доступ к личным данным и потенциально обмениваться ими.

«Например, около двух третей может собирать рекламные идентификаторы или файлы cookie, одна треть может собирать адрес электронной почты

пользователя и около четверти может идентифицировать вышку мобильной связи, к которой подключено устройство пользователя, потенциально предоставляя информацию о геолокации пользователя», исследователи написали в исследовании, опубликованном BMJ.

Только 4% приложений, связанных со здоровьем, фактически передавали данные, которые в основном представляли собой имя пользователя и информацию о местоположении.

«Это значительный процент, и его следует рассматривать как нижнюю границу реальной передачи данных, выполняемой приложениями», – добавили они.

Анализ файлов приложения и кода выявил 65 068 операций по сбору данных; в среднем четыре на каждое приложение.

Анализ трафика приложений выявил 3148 передач пользовательских данных через 616 различных приложений. Основные типы данных, собираемых этими приложениями, включают контактную информацию, местоположение пользователя и несколько идентификаторов устройств, таких как IMEI, MAC-адрес и IMSI, который является международным идентификатором мобильного абонента.

Исследование показало, что 87,5% операций по сбору данных и 56% передач пользовательских данных осуществлялись от имени сторонних сервисов, таких как внешние рекламодатели, поставщики услуг аналитики и отслеживания. По их словам, 23% передач пользовательских данных произошло по незащищенным каналам связи.

Было идентифицировано 665 уникальных сторонних организаций, но, по словам исследователей, за большую часть операций по сбору данных отвечали такие компании, как Google, Facebook и Yahoo!.

«Приложения собирали пользовательские данные от имени сотен третьих лиц, при этом на небольшое количество поставщиков услуг приходится большая часть собранных данных», – говорится в исследовании.

Исследователи также обнаружили, что 28% – 5 903 – проанализированных приложений не предлагали никаких текстов политики конфиденциальности, и по крайней мере 25% – 15 480 – передачи пользовательских данных нарушали то, что было заявлено в политиках конфиденциальности.

«Мобильные приложения быстро становятся источниками информации и инструментами поддержки принятия решений как для врачей, так и для пациентов», – заключили исследователи.

«О таких рисках конфиденциальности следует сообщать пациентам, и их можно сделать частью согласия на использование приложения.

«Мы считаем, что компромисс между преимуществами и рисками приложений мобильного здравоохранения следует учитывать при любых технических и политических обсуждениях, касающихся услуг, предоставляемых такими приложениями». ***(Asha Barbaschow. Macquarie Uni researchers find an oversharing of personal data in health apps // ZDNet (https://www.zdnet.com/article/macquarie-uni-researchers-find-an-oversharing-of-personal-data-in-health-apps/). 16.06.2021).***

***

**«Комиссия по ценным бумагам и биржам (SEC) договорилась с First American об утечке миллионов финансовых отчетов и последующем раскрытии информации.**

Объявленное во вторник, мировое соглашение приведет к закрытию дела в обмен на штраф в размере 487 616 долларов и соблюдение приказа о прекращении противоправных действий.

Жалобы SEC касаются раскрытия примерно 885 миллионов финансовых отчетов, связанных с ипотечными сделками еще с 2003 года по 2019 год.

Эксперт по кибербезопасности Брайан Кребс сообщил об этом гиганту недвижимости США 24 мая 2019 года, отметив, что утечка содержала, среди прочего, номера банковских счетов, ипотечные записи, налоговые данные, номера социального страхования и сканированные изображения водительских прав.

Утечка была локализована на веб-сайте First American и была устранена после того, как компания получила уведомление. First American обвинила в серьезном нарушении безопасности «конструктивный дефект», опубликовала 24 мая заявление для прессы и проинформировала комиссию о выявлении уязвимости 28 мая.

Однако SEC заявляет, что действий First American было недостаточно для соблюдения правил раскрытия информации, поскольку «руководители высшего звена, ответственные за публичные заявления», не были проинформированы о «масштабах» нарушения.

«В частности, в постановлении установлено, что высшее руководство First American не было проинформировано о том, что сотрудники службы информационной безопасности компании определили уязвимость несколькими месяцами ранее, но не смогли устранить ее в соответствии с политикой компании», – говорится в сообщении агентства.

В результате SEC заявила, что компания не раскрыла всю уместную и значимую информацию о нарушении регулирующим органам, и обвинила First American в нарушении мер и процедур раскрытия информации в соответствии с Правилом 13a-15 (a) Закона о биржах (.PDF)…». ***(Charlie Osborne. SEC settles with First American over massive leak of mortgage data, disclosure // ZDNet (https://www.zdnet.com/article/sec-settles-with-first-american-over-massive-leak-of-mortgage-data/). 16.06.2021).***

***

**«Volkswagen обнаружил утечку данных, затронувшую более 3,3 миллиона клиентов.**

Большинство пострадавших являются нынешними или потенциальными покупателями автомобилей Audi. 163 000 человек находятся в Канаде, остальные – в США.

В пятницу автопроизводитель заявил, что сборник данных, использованный для продаж и маркетинга в период с 2014 по 2019 год, был оставлен незащищенным и открыт онлайн «в какой-то момент» в период с августа 2019 года по май 2021 года, хотя точные сроки не установлены.

Ассоциированный поставщик был определен как источник нарушения, но компания не была названа.

Audi и Volkswagen предупредили, что 10 марта к этой информации могла получить доступ «неавторизованная третья сторона».

Volkswagen утверждает, что в результате взлома могли быть раскрыты имя и фамилия, личные и / или служебные почтовые адреса, адреса электронной почты и номера телефонов, а также информация о «приобретенных, арендованных или запрошенных транспортных средствах», например, о транспортных средствах. Идентификационные номера, марки, модели, годы и цвета.

Volkswagen проинформировал соответствующие органы и правоохранительные органы об утечке данных.

Reuters сообщает, что регулирующим органам сообщили, что большинство записей относится только к телефонным номерам и адресам электронной почты, однако примерно 90 000 клиентов Audi и потенциальных покупателей в США могли иметь скомпрометированные данные о праве на покупку и аренду, такие как номера водительских прав, даты о рождении, номера социального страхования, номера счетов или ссуд и налоговые идентификационные номера.

Лицам, чьи конфиденциальные данные были раскрыты, будет предложен бесплатный кредитный мониторинг с помощью регистрационного кода.

Компания заявляет, что кто-либо уведомлял, но не предлагал этот код, не располагал конфиденциальной информацией, и поэтому должен быть готов к появлению фишинговых писем или спама, основанных на утечке каких-либо основных данных.

Электронные письма или письма также могут быть отправлены участникам инцидента безопасности, которые не были прямыми клиентами или потенциальными покупателями.

«В ограниченном числе случаев клиент Audi или Volkswagen или заинтересованный покупатель предоставил имена и контактную информацию для родственника или личной ссылки авторизованному дилеру с целью поиска какого-либо финансирования», – сообщает партнер по уведомлению IDX.

Volkswagen заявляет, что к расследованию инцидента были привлечены внешние эксперты по кибербезопасности.

«Audi и Volkswagen работают со сторонними экспертами по кибербезопасности, чтобы оценить эту ситуацию и отреагировать на нее, и предприняли шаги для решения этой проблемы с вовлеченным поставщиком», – заявляют компании.

Помощь ступица была создана IDX для тех, кто считает, что они оказали влияние на данные нарушения». ***(Charlie Osborne. Volkswagen, Audi disclose data breach impacting over 3.3 million customers, interested buyers // ZDNet (https://www.zdnet.com/article/volkswagen-audi-disclose-data-breach-impacting-over-3-3-million-customers-interested-buyers/). 14.06.2021).***

***

**«К половине учетных записей, скомпрометированных в результате фишинговых атак, доступ осуществляется вручную в течение 12 часов после**

**утечки имени пользователя и пароля, поскольку киберпреступники стремятся как можно быстрее использовать украденные учетные данные.**

Исследователи кибербезопасности из Agari поместили тысячи учетных данных, которые выглядели так, как будто они принадлежали реальным пользователям, но на самом деле находились под контролем исследователей, на веб-сайты и форумы, популярные для сбрасывания украденных имен пользователей и паролей.

Фальшивые учетные данные, засеянные в течение шести месяцев, были разработаны так, чтобы выглядеть как взломанные учетные записи для известных облачных программных приложений.

Исследователи обнаружили, что доступ к учетным записям осуществляется в течение нескольких часов после публикации учетных данных на фишинговых веб-сайтах и форумах.

«Около половины учетных записей были открыты в течение 12 часов после того, как мы фактически загрузили сайты. Доступ к 20% осуществляется в течение часа, а к 40% – в течение шести часов. Это действительно показывает, насколько быстро взломанная учетная запись используется», – Крейн Хассолд Старший директор по исследованию угроз Agari сообщил ZDNet.

Доступ практически ко всем учетным записям осуществлялся вручную. Это может быть рутинной задачей, но в конечном итоге она оказывается полезной для киберпреступников, поскольку они могут точно проверить, действительно ли учетные данные работают.

«Я уверен, что с их стороны это довольно утомительный процесс, но они получают много полезной информации и используют учетные записи различными способами для различных типов злонамеренных действий», – сказал Хассолд.

Например, получая доступ к учетной записи, злоумышленник может попытаться найти конфиденциальную информацию в почтовых ящиках людей или даже в их программном облачном хранилище, которое может быть украдено и использовано для дальнейших атак или продано.

Также существует вероятность того, что злоумышленники могут использовать скомпрометированные учетные записи для проведения других атак, таких как фишинг или атаки компрометации корпоративной электронной почты (BEC), используя скомпрометированную учетную запись для запуска дальнейших кампаний.

Один злоумышленник попытался использовать скомпрометированную учетную запись для проведения атак BEC на сектор недвижимости, запустив электронные письма, в которых жертвы пытались перенаправить на веб-сайт для кражи данных для входа в компании, занимающиеся недвижимостью. Однако в этом случае, поскольку фальшивые учетные данные контролировались исследователями, ни одно из отправленных электронных писем фактически не пришло по назначению.

Однако он демонстрирует, как киберпреступники берут скомпрометированные учетные данные и пытаются использовать их, чтобы получить доступ к дополнительным учетным записям.

«Фишинг с учетными данными ведет к взлому учетной записи, что ведет к большему количеству фишинговых кампаний с учетными данными, что ведет к увеличению количества скомпрометированных учетных записей и так далее», – сказал Хассолд.

Несмотря на то, что доступ к скомпрометированным учетным записям осуществляется быстро, исследование показало, что от них часто отказываются примерно через неделю – хотя к этому времени, вероятно, это связано с тем, что злоумышленники перешли на другие учетные записи, возможно, после использования исходной учетной записи в качестве ступеньки для доступа к ним.

Организации могут принимать меры предосторожности, чтобы защитить своих пользователей, облачные приложения и сеть в целом от фишинга и других атак. Один из них – наличие соответствующих средств защиты, таких как антивирусное программное обеспечение или фильтр спама.

Между тем, использование многофакторной аутентификации может помочь предотвратить использование взломанных учетных записей, так как это значительно усложняет использование злоумышленником, а также предупреждает жертву о том, что что-то не так». ***(Danny Palmer. This is how fast a password leaked on the web will be tested out by hackers // ZDNet (https://www.zdnet.com/article/this-is-how-fast-a-password-leaked-on-the-web-will-be-tested-out-by-hackers/). 08.06.2021).***

***

**«COVID-19 показал высокую ценность личных данных для предприятий по всему миру, а также подчеркнул их уязвимость для злоупотреблений и атак.** В ответ страны пересмотрели свои законы о конфиденциальности и защите данных. В Южной Африке Закон о киберпреступности и кибербезопасности и Закон о защите личной информации – это новые законы, которые приведут законодательство страны о защите данных и кибербезопасности в соответствие с мировыми стандартами. В других странах Африки действуют аналогичные законы, но в большинстве из них отсутствуют законы о конфиденциальности данных. Учитывая нынешний быстрый переход к бизнес-моделям, ориентированным на цифровые технологии, внедрение этих правовых средств защиты и рекомендаций в Африке стало неотложной задачей.

Пандемия продемонстрировала высокую ценность персональных данных для мировой экономики, а также подчеркнула их уязвимость для злоупотреблений и атак. В ответ правительства всего мира пересматривают свои законы и постановления о конфиденциальности и защите данных, в том числе в Южной Африке. Компания Kaspersky, занимающаяся глобальной кибербезопасностью, недавно отметила рост числа кибератак в африканских странах, особенно в ключевых финансовых центрах Южной Африки, Кении и Нигерии. Фирма, занимающаяся кибербезопасностью, отметила, что быстро развивающиеся цифровые технологии привели к повышенному риску сложных постоянных угроз и мероприятий по наемному взлому в Африке.

*Южная Африка*

В Южной Африке Закон о киберпреступности и кибербезопасности (Закон) был подписан президентом ЮАР Сирилом Рамафосой в начале июня 2021 года,

приведя законодательство страны в области кибербезопасности в соответствие с мировыми стандартами. Закон обязывает поставщиков услуг электронной связи и финансовые учреждения действовать, когда они узнают, что их компьютерные системы были вовлечены в нарушение кибербезопасности, как определено в Законе. Согласно закону, они должны сообщать о таких правонарушениях в Южноафриканскую полицейскую службу в течение 72 часов после того, как стало известно о правонарушении, и сохранять любую информацию, которая может помочь в расследовании. Несоблюдение этого положения является уголовным преступлением и может быть наложено крупными штрафами.

Закон также предусматривает уголовную ответственность за вредоносные сообщения с данными, например, сообщения, призывающие к насилию или нанесение ущерба имуществу, или угрозы, а также сообщения, содержащие интимные изображения. В Законе данные в широком смысле определяются как «электронные представления информации в любой форме». Закон также предусматривает уголовную ответственность за кибермошенничество, вымогательство, подлог и кражу нематериального имущества. Также преступлением считается незаконный доступ к компьютерной системе, носителю данных или личным данным. Виновным в нарушении кибербезопасности грозит крупный штраф и длительное тюремное заключение сроком до 15 лет.

В Южной Африке безопасность данных также регулируется Законом о защите личной информации (POPIA). 1 июля 2021 года основные положения POPIA вступят в силу. Этот закон, среди прочего, способствует защите личной информации, обрабатываемой государственными и частными организациями, очерчивает права субъектов данных, регулирует трансграничный поток личной информации, вводит обязательные обязательства сообщать и уведомлять о случаях утечки данных и налагает предусмотренные законом штрафы за нарушение закона.

Одним из условий законной обработки с точки зрения POPIA является использование мер безопасности, которые предписывают, что целостность и конфиденциальность личной информации должны быть обеспечены лицом, контролирующим эту информацию. Это предписано POPIA для предотвращения потери, повреждения, несанкционированного доступа или уничтожения личной информации.

POPIA также обязывает лиц, ответственных за обработку личной информации, сообщать о любом незаконном доступе к личной информации (утечке данных) Регулятору информации в течение разумного периода времени. Как и Закон о кибербезопасности, POPIA приводит Южную Африку в соответствие с международными законами о защите данных, регулируя обработку личной информации физических и юридических лиц и возлагая более обременительные обязательства на «ответственные стороны», которые обрабатывают такую информацию.

Что касается POPIA, когда есть разумные основания полагать, что к личной информации субъекта данных был получен доступ или получен каким-либо неавторизованным лицом, ответственная сторона должна уведомить Регулятор информации, а также субъект данных, если только это лицо не личность не может быть установлена.

Уведомление должно быть сделано как можно скорее после обнаружения компрометации с учетом потребностей правоохранительных органов или любых мер, необходимых для определения масштабов компрометации и восстановления целостности информационной системы ответственной стороны. Ответственная сторона может отложить уведомление субъекта данных только в том случае, если государственный орган, ответственный за предотвращение, обнаружение или расследование правонарушений, или регулятор информации, определит, что это будет препятствовать уголовному расследованию.

Уведомление должно быть в письменной форме и отправлено либо по электронной почте, либо отправлено на последний известный адрес субъекта данных. Уведомление также может быть размещено на видном месте на веб-сайте ответственной стороны, опубликовано в средствах массовой информации или в соответствии с указаниями регулятора информации. Он должен предоставлять достаточно информации, чтобы позволить субъекту данных принять меры защиты от потенциальных последствий компрометации.

Кроме того, Регулятор информации может дать указание ответственной стороне предать гласности любым указанным способом факт любого нарушения целостности или конфиденциальности личной информации, если есть разумные основания полагать, что такая гласность защитит субъекта данных.

Организация, вовлеченная в ситуацию утечки данных, также может быть подвергнута административному штрафу, штрафу или санкциям, либо гражданским искам и / или групповым искам.

*Гана*

В 2020 году Гана аналогичным образом приняла Закон о кибербезопасности 2020 года, чтобы контролировать реакцию страны на предотвращение инцидентов, связанных с кибербезопасностью, и управление ими. Закон учреждает Управление кибербезопасности и обеспечивает защиту критически важной информационной инфраструктуры страны. Закон также регулирует деятельность в области кибербезопасности, контролирует защиту детей в Интернете и направлен на развитие экосистемы кибербезопасности Ганы.

Однако законы о конфиденциальности данных, которые регулируют, помимо прочего, безопасность данных и нарушения, в настоящее время действуют менее чем в половине африканских стран. На региональном уровне в Сообществе по вопросам развития юга Африки и Экономическом сообществе западноафриканских государств действуют политики защиты данных, и на этот континент также распространяется Конвенция Африканского союза о кибербезопасности и личных данных (2014 г.) (Конвенция). По состоянию на май 2020 года Конвенцию ратифицировали только восемь из 55 членов Африканского союза (Ангола, Гана, Гвинея, Маврикий, Мозамбик, Намибия, Руанда и Сенегал), в то время как 14 стран подписали, но не ратифицировали ее. Южная Африка, Кения и Нигерия еще не подписали Конвенцию.

Законодательство, регулирующее цифровую экономику, имеет важное значение для защиты африканских граждан с точки зрения как их прав на цифровую конфиденциальность, так и угроз кибербезопасности, и в то же время гарантирует, что их онлайн-свободы не будут поставлены под угрозу. АС поощряет

свои государства-члены подписать Конвенцию и внедрить сбалансированное местное законодательство, которое имеет полную юридическую силу и уважает права человека.

Чтобы облегчить этот процесс, консультации с заинтересованными сторонами в правительстве, предприятиями (местными и международными) и организациями, представляющими общество в целом, обеспечат сбалансированный подход при разработке этих законов. Международное законодательство следует рассматривать наряду с местными законами, учитывая безграничный характер онлайн-среды, а консультации с экспертами по технологиям по вопросам политики означают, что можно должным образом учитывать специфику этого быстро развивающегося сектора. Принимая во внимание текущий быстрый переход к цифровым бизнес-моделям, внедрение этих правовых средств защиты и рекомендаций стало неотложной задачей для всех африканских стран». ***(Africa: Implementation of cybersecurity and data protection law urgent across continent // Baker & McKenzie (https://insightplus.bakermckenzie.com/bm/viewContent.action?key=Ec8teaJ9Varwrjqjy7WjKl7eOOGbnAEFKCLORG72fHz0%2BNbpi2jDfaB8lgiEyY1JpGSGsLXap4O6bJK6KF1TgA%3D%3D&nav=FRbANEucS95NMLRN47z%2BeeOgEFCt8EGQ0qFfoEM4UR4%3D&emailtofriendview=true&freeviewlink=true). 07.06.2021).***

***

**«4 июня 2021 года Европейская комиссия приняла и опубликовала новый набор так называемых стандартных договорных положений (SCC), обеспечивающих правовую основу для международной передачи персональных данных из ЕС / ЕЭЗ в третьи страны.** Эти SCC являются долгожданным обновлением стандартных договорных положений (один установлен в 2004 и 2001 годах, а другой – в 2010 году), принятых в соответствии с Директивой ЕС о защите данных 95/46 / ЕС, которые на практике были основным средством обеспечения международная передача персональных данных. Новые SCC включают требования Общего регламента ЕС по защите данных (GDPR) и учитывают решение Суда Европейского Союза (CJEU) от июля 2020 года по делу Schrems II.

В отличие от предыдущих документов, новые SCC стремятся охватить четыре сценария передачи в одном документе, а именно:

• Контроллеры в ЕС / ЕЭЗ передают личные данные контроллерам за пределами ЕС / ЕЭЗ;

• Контроллеры в ЕС / ЕЭЗ, передающие личные данные обработчикам за пределами ЕС / ЕЭЗ;

• Обработчики в ЕС / ЕЭЗ, передающие личные данные (суб) обработчикам за пределами ЕС / ЕЭЗ;

• Обработчики в ЕС / ЕЭЗ передают персональные данные контроллерам за пределами ЕС / ЕЭЗ.

Новые SCC вступят в силу через 20 дней после публикации в Официальном журнале Европейского Союза. Старое решение о внедрении SCC будет отменено через три месяца после этой даты, поэтому экспортеры данных, внедряющие новые

механизмы, должны использовать новые SCC не позднее, чем через три месяца после публикации. Экспортеры данных, использующие (подписанные) старые SCC, могут продолжать полагаться на них еще в течение 15 месяцев (всего 18 месяцев с момента публикации в Официальном журнале), пока операции обработки остаются неизменными.

*Первоначальные наблюдения*

Хотя SCC содержат множество новых элементов, в которые стоит погрузиться, ниже мы выделяем несколько основных:

• Как и текущие SCC, новые SCC достигнут цели по обеспечению правовой основы для международной передачи персональных данных только в том случае, если в их текст, пункт 2 (а) не будет внесено никаких изменений.

• Субъекты данных как сторонние бенефициары могут задействовать и обеспечить соблюдение существенного числа положений SCC, пункт 3.

• SCC требуют, чтобы применимым законодательством был закон государства-члена ЕС (статья 17), а споры разрешались в судах государства-члена ЕС (статья 18). Пункт 12 содержит формулировку обязательной ответственности и возмещения убытков.

• Существует также новое «закрепляющее» положение (раздел 7), позволяющее субъекту, который (еще) не является стороной SCC, присоединиться к этим пунктам в качестве экспортера или импортера данных. Этот новый механизм будет особенно полезен в контексте приобретений, дополнительных юридических лиц и субпроцессоров.

• Пункт 14 касается местных законов и практики, влияющих на соблюдение SCC, и требует подробной оценки и документирования законов в стране импортера данных. Для американских компаний, выступающих в качестве импортеров данных, пункт 14, сноска 12 будет особенно важен. В сноске 12 SCC заявляют, что «различные элементы могут рассматриваться как часть общей оценки. Такие элементы могут включать соответствующий и задокументированный практический опыт с предыдущими случаями запросов на раскрытие информации от государственных органов или отсутствие таких запросов, охватывающих достаточно репрезентативные временные рамки». В сноске 12 поясняется, что, когда рассматривается такой практический опыт, он должен подкрепляться «другими соответствующими, объективными элементами», которые необходимо оценивать на предмет надежности и репрезентативности.

• Если у импортера данных есть основания полагать, что он не сможет соблюдать SCC, он должен сообщить об этом экспортеру данных. Затем экспортер данных должен определить соответствующие меры для исправления ситуации. Если такие соответствующие меры предосторожности не могут быть реализованы, экспортер данных должен приостановить передачу. Кроме того, если импортер данных получает «юридически обязательный запрос» от государственного органа о раскрытии переданных личных данных, он должен проинформировать экспортера данных и субъект данных, где это возможно. Сводная информация также должна периодически предоставляться экспортеру данных.

• Пока нет полной картины относительно того, будет ли достаточно внедрения SCC для создания достаточно прочной правовой основы для

международных переводов. Как и старые SCC, новые SCC «считаются обеспечивающими надлежащие гарантии» для передачи персональных данных от экспортеров данных, подпадающих под действие GDPR, импортерам данных, не подпадающим под действие GDPR, статья 46 (1) GDPR. В Шремсе II, CJEU постановил, что контролерам и обработчикам при использовании SCC, возможно, придется внедрить дополнительные меры безопасности для обеспечения адекватной защиты персональных данных, передаваемых в соответствии с SCC, поскольку статья 46 GDPR также требует, чтобы «были доступны обеспеченные правовой санкцией права субъектов данных и эффективные средства правовой защиты…» В пункте 2 (a) SCC Европейская комиссия заявляет, что SCC устанавливают «соответствующие гарантии, включая обеспеченные правовой санкцией права субъектов данных и эффективные средства правовой защиты», поэтому могут быть аргументы в пользу того, что дополнительных мер не требуется, помимо тех, которые уже предусмотрены SCC. требовать. На этом фоне обновление «Рекомендаций EDPB 01/2020 о мерах, которые дополняют инструменты передачи данных для обеспечения соответствия уровню защиты персональных данных ЕС», Которая может быть завершена уже 18 июня 2021 года.

*Дополнительные примечания*

Наряду с SCC, Европейская комиссия также выпустила стандартные договорные положения в соответствии со статьей 28 GDPR для контроллеров и процессоров в ЕС / ЕЭЗ (по сути, шаблон соглашения об обработке данных).

Управление Комиссара по информации Соединенного Королевства объявило в мае 2021 года, что оно работает над индивидуальным набором стандартных договорных положений для использования в контексте переводов из Соединенного Королевства.

*Следующие шаги*

Новые SCC требуют более детальной оценки и обязательств по документации для международной передачи персональных данных. Поэтому компаниям следует в ближайшее время начать инвентаризацию своих существующих стандартных договорных положений с целью перехода на новые SCC в течение 18-месячного срока.

Кроме того, для импортеров данных в Соединенных Штатах будет важно продолжать уделять пристальное внимание возможной разработке преемника программы Privacy Shield между ЕС и США». ***(European Commission adopts and publishes new Standard Contractual Clauses for international transfers of personal data // WilmerHale (https://www.wilmerhale.com/en/insights/blogs/WilmerHale-Privacy-and-Cybersecurity-Law/20210607-european-commission-adopts-and-publishes-new-standard-contractual-clauses-for-international-transfers-of-personal-data#page=1). 07.06.2021).***

***

**«Китайская торговая операция Alibaba Taobao пострадала от утечки данных более чем на миллиард точек данных, включая имена пользователей и номера мобильных телефонов.** Информация была взята с сайта поисковым роботом, разработанным партнером по маркетингу.

Китайское издание 163.com сообщило об этом случае на прошлой неделе, а сегодня о нем сообщил Wall Street Journal.

В обоих отчетах говорится, что разработчик создал поискового робота, способного проникать в глубину информации, доступной человеческому глазу на Taobao, и что он проработал несколько месяцев, прежде чем Alibaba заметила это усилие.

163.com предполагает, что источником поискового робота была компания, которая зарабатывает деньги на партнерских рефералах на Taobao, и что сайт был очищен с ноября 2019 года до тех пор, пока Alibaba не заметила активность в июле 2020 года. Alibaba уведомила власти, начато расследование, и дело попал в Народный суд района Суйян, который в мае признал разработчика и его работодателя виновными в изъятии данных.

Оба были приговорены к трем годам заключения.

К счастью, преступники, похоже, не делились данными, а копили их для своих целей.

Новости об инциденте со сканированием приходят, когда Китай все активнее пытается обуздать своих веб-гигантов, не дать им получить чрезмерную рыночную власть и гарантировать, что они не собирают больше данных, чем необходимо для их повседневной деятельности.

В этом случае суд установил, что Alibaba и Taobao не нарушали законов. Компании еще могут столкнуться с санкциями за слабость, поскольку веб-сканеры далеко не неизвестны или их невозможно предвидеть.

Сообщается, что Alibaba «призналась в провале» – подход, совершенно отличный от того, который демонстрирует Facebook, когда в апреле 2021 года вновь появились новости о более чем 500 миллионах очищенных клиентских записей, а в Social Network ™ пользователям было предложено пересмотреть свои настройки конфиденциальности, чтобы остановить парсеры». ***(Simon Sharwood. Alibaba suffers billion-item data leak of usernames and mobile numbers // The Register (https://www.theregister.com/2021/06/16/alibaba_tabao_scraped_data_leak/). 16.06.2021).***

***

**«Европейская комиссия подаст судебный иск против Бельгии после жалоб на то, что ее регулятор защиты данных не соответствует требованиям независимости ЕС, по словам трех человек, знакомых с процессом.**

По словам людей, в среду будет объявлен судебный иск, формально известный как процедура нарушения прав. Судебное разбирательство является ответом на анонимные жалобы, поданные в прошлом году, в которых утверждалось, что способность бельгийского регулятора конфиденциальности действовать независимо находится под угрозой, поскольку некоторые из его членов также связаны с правительством.

Закон ЕС о конфиденциальности, Общий регламент по защите данных (GDPR), требует, чтобы регулирующие органы были независимыми от правительства.

Чтобы официально начать разбирательство, Комиссия отправит письмо с официальным уведомлением в Бельгию с запросом дополнительной информации, на которую страна должна ответить в течение определенного периода, который обычно составляет два месяца. В конечном итоге дело может быть передано в Суд Европейского Союза, хотя большинство дел разрешается до этого этапа.

В одной из жалоб, поданных в ноябре, говорилось, что решение регулирующего органа включить трех должностных лиц, которые также подотчетны правительственным министрам, в комиссию, дающую заключения по законопроектам, нарушает требования GDPR для членов, чтобы они «оставались свободными от внешнего влияния».

Хотя двое из них с тех пор отказались, одно должностное лицо, Фрэнк Роббен, который возглавляет многие инициативы страны в области публичных данных, сохраняет свою роль в регулирующем органе.

В жалобах также высказывались возражения против четвертого члена той же комиссии, Барта Пренила, за его членство в правительственном комитете, который разрешает определенный обмен данными в государственном секторе. Пренил также остается в своей роли.

Сам комитет обвиняется в отдельной жалобе в Комиссию, поданной в июле, в нарушении ограничений GDPR на предварительное одобрение проектов, связанных с персональными данными.

И Роббен, и Пренил отрицали, что их позиция ставит под угрозу независимость регулирующего органа.

В прошлом году бельгийский регулятор по защите данных заявил, что назначение официальных лиц соответствовало критериям, изложенным в GDPR, и что сами люди заявили об отсутствии каких-либо конфликтов интересов.

Но два директора регулятора дистанцировались от заявления, подчеркнув продолжающиеся разногласия между высшими должностными лицами регулятора». ***(VINCENT MANANCOURT. EU to take legal action targeting Belgian privacy regulator // Politico (https://www.politico.eu/article/eu-to-take-legal-action-targeting-belgian-privacy-regulator/). 08.06.2021).***

***

**«Сообщения об утечке данных TurboTax были преувеличены, согласно Intuit, которая владеет платформой для подготовки налогов.**

Несколько новостных агентств недавно сообщили, что неопределенное количество учетных записей TurboTax было взломано в результате волны атак по подбору учетных данных. В подобных атаках используются учетные данные, украденные с других веб-сайтов и повторно используемые на сайте TurboTax.

«Нарушений систем Intuit не было», – сказал официальный представитель компании Рик Хейнеман.

Он пояснил, что Intuit уведомила одного клиента в Массачусетсе, что заблокировала его учетную запись после обнаружения попытки несанкционированного доступа к ней.

«Затем мы передали копию этого уведомления одному человеку с местными властями», – сказал он TechNewsWorld.

Когда группы предотвращения мошенничества Intuit замечают попытку или успешный вход в учетную запись Intuit, которая использовала собранные учетные данные из сторонних источников, как заметил Хейнеман, мы немедленно блокируем доступ к этой учетной записи, отправляем уведомление клиенту, требуем процесс проверки личности владельцем учетной записи и попросите изменить свои учетные данные, чтобы повторно получить доступ к учетной записи.

«Intuit осуществляет надежные процессы предотвращения мошенничества в режиме реального времени, в том числе при входе в систему и в продукте, – для выявления любого предполагаемого аномального поведения», – сказал он.

Он добавил, что для защиты информации о клиентах компания внедрила ряд организационных, технических и административных средств контроля для своих продуктов и услуг. Они включают в себя многофакторную аутентификацию, шифрование и надежные возможности регистрации, мониторинга и блокировки.

*Прибыльная тактика*

Bleeping Computer в субботу сообщил, что Intuit уведомила клиентов TurboTax о том, что злоумышленники получили доступ к некоторой их личной и финансовой информации после того, что выглядело как серия атак по захвату учетных записей.

Аналогичный отчет появился в понедельник на сайте TechRadar. Производитель финансового программного обеспечения Intuit уведомил пользователей своей платформы TurboTax о том, что злоумышленники получили доступ к некоторой их личной и финансовой информации в ходе серии атак по захвату аккаунтов.

Атака с заполнением учетных данных на таком сайте, как TurboTax, может быть очень прибыльной, отмечает Джеймс Маккуигган, защитник осведомленности в KnowBe4, учебном центре по кибербезопасности в Клируотере, штат Флорида.

«Он обеспечивает доступ к личной информации о пользователях, их налоговой информации и, конечно же, их номерам социального страхования для них и, возможно, их ближайших родственников», – сказал он TechNewsWorld.

«Имея более 8,4 миллиона паролей в дикой природе и более 3,5 миллиардов этих паролей, привязанных к реальным адресам электронной почты, он обеспечивает отправную точку для киберпреступников, чтобы атаковать различные онлайн-сайты, которые используют учетные записи своих клиентов», – продолжил он.

«Если пользователи создают учетные записи с ранее раскрытыми паролями, они упрощают киберпреступникам возможность кражи их данных», – сказал он.

«Проведение атак с заполнением учетных данных легко, с низким уровнем риска и в случае успеха обеспечивает высокую окупаемость инвестиций», – добавил Лео Пейт, консультант по безопасности приложений из nVisium, поставщика безопасности приложений в Херндоне, штат Вирджиния.

«С преступной точки зрения, многие платформы не предлагают строгих мер безопасности, таких как многофакторная аутентификация, или пользователи просто не пользуются ими, даже если они доступны, что приводит к более высокому уровню успешной компрометации», сказал он TechNewsWorld.

*Используйте уникальные пароли*

Несмотря на предупреждения о повторном использовании паролей, потребители продолжают эту практику. «От старых привычек трудно избавиться», – заметил Маккуигган.

«Например, – продолжил он, – людям не нравится придумывать разные пароли для каждой учетной записи. Им легче использовать тот, который они легко запомнили, или добавить к нему какие-то вариации, например, другой номер или название веб-сайта».

«Потребители сегодня использовать десятки услуг в Интернете. Имея уникальный надежный пароль для каждой службы в чьей – то голове практически невозможно из – за различные требования сложности, требование длиной, и само количество услуг, потребляемым,» добавил Бен Eichorst, главный инженер Yubico, из Пало-Альто, Калифорния, производителя решений для USB и беспроводной аутентификации.

Он сообщил TechNewsWorld, что недавнее исследование показывает, что 51 процент респондентов, ответивших на вопросы ИТ-безопасности, заявили, что их организации подверглись фишинговой атаке, а еще 12 процентов респондентов заявили, что их организации испытали кражу учетных данных. Тем не менее, только 53% респондентов, ответивших на вопросы ИТ-безопасности, заявили, что их организации изменили способ управления паролями или защищенными корпоративными учетными записями.

«Интересно, – продолжил он, – что люди повторно используют пароли в среднем для 16 учетных записей рабочих мест, и респонденты, отвечающие за ИТ-безопасность, говорят, что они повторно используют пароли в среднем для 12 учетных записей рабочих мест».

*Защита пользователей и бизнеса*

Алекса Слингер, эксперт по управлению идентификацией из OneLogin, производителя облачных решений для управления идентификацией и доступом в Сан-Франциско, отметила, что с ростом количества утечек данных растет и количество украденных учетных данных.

«Несмотря на постоянное освещение взломов в СМИ, пользователи продолжают повторно использовать пароли и подвергать организации риску», – сказала она TechNewsWorld. «Чтобы защитить своих пользователей и свой бизнес, организациям следует принять дополнительные меры безопасности».

Такие меры могут включать:

Ограничение количества запросов аутентификации за сеанс, чтобы снизить скорость атак ботов с заполнением учетных данных.

Предложение или требование настройки многофакторной аутентификации, которая потребует от злоумышленника другой формы идентификации, кроме украденных учетных данных.

Используйте проверку скомпрометированных учетных данных, чтобы предупредить и предотвратить использование пользователем взломанной информации для входа.

*Вас уговорили*

В последнее время потребители начали получать предупреждения, когда один из их паролей появляется в кеше украденных данных. «Пользователи,

которые решили хранить и генерировать свои пароли с помощью безопасного менеджера паролей, могут получать уведомления об известных нарушениях», – сказал Эйхорст.

«Одна из основных ценностей диспетчера паролей заключается в том, что он сообщит вам, какие из ваших учетных записей в Интернете были взломаны», – добавил Крис Хазелтон, директор по решениям безопасности Lookout, поставщика мобильных фишинговых решений в Сан-Франциско.

«Это также может автоматизировать процесс смены пароля, что позволит вам быстрее реагировать на взлом», – сказал он TechNewsWorld.

Эйхорст добавил, что отдельные компании, работающие в Интернете, улучшают свои методы проверки паролей, чтобы запретить утечку известных паролей.

Однако это пока еще не обычная практика. «Уведомления, безусловно, более распространены, но эти уведомления представляют собой всего лишь руководство, и пользователям не запрещается продолжать использовать эти взломанные пароли», – отметил Дэвид Стюарт, генеральный директор компании Approov из Эдинбурга в Великобритании, которая выполняет динамическую динамику на двоичном уровне. анализ программного обеспечения.

«Следует рассмотреть вопрос о том, следует ли блокировать доступ пользователей к службам до тех пор, пока они не обновят взломанный пароль», – сказал он TechNewsWorld. «В настоящее время это очень редко, но кажется разумным шагом».

Потребители, обеспокоенные тем, что их пароли были скомпрометированы, также могут быть более активными, запустив проверку своих паролей на веб-сайте HaveIBeenPwned, который отслеживает адреса электронной почты и номера телефонов, которые подвергались утечке данных за последние пятнадцать лет». ***(John P. Mello Jr. Reports of TurboTax Breach Greatly Exaggerated // ECT News Network, Inc (https://www.technewsworld.com/story/87168.html). 16.06.2021).***

***

**«Carnival Corporation, крупнейший в мире оператор круизных судов, раскрыла утечку данных после того, как злоумышленники получили доступ к некоторым из ее ИТ-систем, а также к личной, финансовой и медицинской информации, принадлежащей клиентам, сотрудникам и членам экипажа.**

Carnival входит в индексы фондовых рынков S&P 500 и FTSE 100, в нем работает более 150 000 сотрудников примерно в 150 странах, и ежегодно он обеспечивает поездки для отдыха примерно 13 миллионам гостей.

Компания управляет девятью ведущими мировыми брендами круизных линий (Carnival Cruise Line, Costa, P&O Australia, P&O Cruises, Princess Cruises, Holland American Line, AIDA, Cunard и Seabourn) и туристической компанией (Holland America Princess Alaska Tours).

*Предупреждение о риске неправильного использования данных*

«Несанкционированный доступ третьих лиц к ограниченному количеству учетных записей электронной почты был обнаружен 19 марта 2021 года», –

говорится в письме с уведомлением об утечке данных, которое недавно было отправлено пострадавшим клиентам.

Однако старший вице-президент и директор по связям с общественностью Carnival Роджер Фриззелл сообщил BleepingComputer после публикации статьи, что злоумышленники получили доступ к «ограниченным частям его систем информационных технологий».

«Похоже, что в середине марта неавторизованная третья сторона получила доступ к определенной личной информации, касающейся некоторых наших гостей, сотрудников и экипажа.

«Затронутая информация включает данные, которые обычно собираются в процессе работы с гостями и бронирования путешествий, а также в процессе работы или предоставления услуг Компании, включая COVID или другие тесты безопасности».

Согласно Carnival, доступная информация включала имена, адреса, номера телефонов, номера паспортов, даты рождения, информацию о здоровье и, в некоторых ограниченных случаях, дополнительную личную информацию, такую как номера социального страхования или национальные идентификационные номера.

Оператор круизной линии также предупредил пострадавших клиентов, сотрудников, а также Carnival Cruise Line, Holland America Line, Princess Cruises и медицинский персонал, что они обнаружили доказательства, указывающие на «низкую вероятность неправомерного использования данных».

*Дважды атакован программой-вымогателем за год*

BleepingComputer ранее сообщал, что в августе 2020 года на Carnival также произошла атака с использованием программ-вымогателей, инцидент, подтвержденный оператором круизной линии в форме 8-K, поданной в Комиссию по ценным бумагам и биржам США (SEC).

Два месяца спустя Carnival сообщил в отдельной SEC, что группа вымогателей, стоявшая за августовской атакой, получила доступ к личной информации как клиентов, так и сотрудников во время атаки.

Согласно информации, поданной Carnival в Генеральную прокуратуру штата Мэн, от августовской атаки с использованием программ-вымогателей пострадало около 37 500 человек.

Атака программы-вымогателя в августе произошла после утечки данных, раскрытой в марте 2020 года, которая также привела к раскрытию личной и финансовой информации клиентов после того, как злоумышленники получили доступ к учетным записям электронной почты сотрудников Carnival.

Согласно форме 10-Q, поданной в SEC в апреле 2021 года, в декабре 2020 года Carnival подверглась второй (ранее не разглашаемой) атаке с использованием программ-вымогателей, «фазы расследования и исправления» все еще продолжаются.

«В настоящее время нет никаких указаний на какое-либо неправомерное использование информации, потенциально доступной или полученной, и мы продолжаем работать с регулирующими органами, чтобы довести до конца эти

вопросы и другие инциденты, о которых необходимо сообщить», – сказал Карнавал об инциденте с вымогателем в декабре 2020 года.

BleepingComputer сообщал в то время, что немецкая круизная линия и дочерняя компания Carnival AIDA Cruises столкнулись с загадочными «ИТ-ограничениями», которые привели к отмене их новогодних круизов.

Costa Crociere, еще одна дочерняя компания Carnival, также пострадала от отключения ИТ-инфраструктуры в связи с атакой программы-вымогателя в декабре, которая помешала клиентам бронировать поездки через систему онлайн-бронирования круизной линии…». ***(Sergiu Gatlan. Carnival Cruise hit by data breach, warns of data misuse risk // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/carnival-cruise-hit-by-data-breach-warns-of-data-misuse-risk/). 17.06.2021).***

***

**«Крупнейший поставщик пропана в Америке, AmeriGas, сообщил об утечке данных, которая длилась недолго, но затронула 123 сотрудника.**

Компания AmeriGas обслуживает более 2 миллионов клиентов во всех 50 штатах США и имеет более 2500 точек распространения.

Об утечке данных в этом месяце пропановый гигант сообщил в Генеральную прокуратуру Нью-Гэмпшира.

Нарушение данных длилось 8 секунд, затронуло 123 сотрудника.

В этом месяце AmeriGas направила письмо с уведомлением об утечке данных в Генеральную прокуратуру Нью-Гэмпшира.

Однако причиной утечки данных является JJ Keller, поставщик, отвечающий за предоставление AmeriGas услуг по соблюдению требований Департамента транспорта (DOT).

Эти услуги включают помощь AmeriGas в проверке водительских прав, тестировании водителей на наркотики и алкоголь и других нормативных проверках, проводимых DOT.

10 мая JJ Keller обнаружил в своих системах подозрительную активность, связанную с учетной записью электронной почты компании.

Таким образом, поставщик незамедлительно начал расследование своей сети, чтобы обнаружить, что сотрудник JJ Keller стал жертвой фишингового электронного письма, что привело к компрометации его учетной записи.

В течение этого короткого окна доступа злоумышленники могут просматривать определенные файлы, находящиеся в скомпрометированной учетной записи сотрудника.

После сброса учетных данных сотрудника Джей Джей Келлер сразу же приступил к судебно-медицинской экспертизе, чтобы определить полный объем этого взлома.

К 21 мая Джей Джей Келлер уведомил AmeriGas о том, что в результате этого восьмисекундного взлома были обнаружены записи 123 сотрудников AmeriGas, которые присутствовали в файлах, доступных злоумышленнику.

«По словам Дж. Дж. Келлера, во время 8-секундного взлома злоумышленник имел доступ к внутренней электронной почте с приложениями к электронным

таблицам, содержащими информацию 123 сотрудников AmeriGas, включая идентификаторы лабораторий, номера социального страхования, номера водительских прав и даты рождения».

«На сегодняшний день нам неизвестно о каком-либо фактическом использовании или попытках неправомерного использования этих персональных данных в результате этого инцидента», – сообщила компания AmeriGas в образце письма с уведомлением о нарушении данных от 4 июня 2021 года.

В результате взлома также была обнаружена информация только об одном жителе Нью-Гэмпшира, который с тех пор был уведомлен об инциденте и получил бесплатные услуги кредитного мониторинга.

В настоящее время нет никаких указаний на то, что какая-либо информация о сотрудниках была скопирована или использована неправильно.

*Второй инцидент с безопасностью, касающийся АмериГаза в этом году*

Этот инцидент стал вторым инцидентом, связанным с утечкой данных, касающимся АмериГаза в этом году.

В марте 2021 года компания AmeriGas раскрыла попытку взлома данных, в результате которой агент по обслуживанию клиентов компании был уволен за возможное неправомерное использование информации о кредитной карте клиента.

Согласно AmeriGas, некоторые клиенты, звонившие в службу поддержки клиентов AmeriGas, устно раскрыли информацию о своей кредитной карте этому представителю, который, возможно, использовал эту информацию для совершения несанкционированных покупок.

В то время компания сказала:

«Недавно мы обнаружили несанкционированное раскрытие информации о кредитной карте одному из наших агентов по обслуживанию клиентов».

«Мы не знаем, была ли предоставлена информация о вашей кредитной карте, но пишем с особой осторожностью».

«Мы исследовали проблему в качестве меры предосторожности, чтобы защитить вашу информацию».

«Участвующий в этом агент был уволен, и мы уже ввели дополнительные меры безопасности», – сообщила компания в то время.

Кибератаки и инциденты против критически важных энергетических компаний продолжают расти, что вызывает необходимость в усилении контроля безопасности и обучении осведомленности в организациях». ***(Ax Sharma. Largest US propane distributor discloses '8-second' data breach // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/largest-us-propane-distributor-discloses-8-second-data-breach/). 15.06.2021).***

***

**«21 июня 2021 года Европейский совет по защите данных («EDPB») опубликовал окончательные Рекомендации 01/2020 о мерах, которые дополняют инструменты передачи для обеспечения соответствия уровню защиты персональных данных ЕС («Рекомендации»).** Эти долгожданные Рекомендации являются чрезвычайно важным шагом для рассмотрения рисков, связанных с передачей данных, и управления соответствием GDPR в организации.

Окончательные рекомендации следуют за проектами рекомендаций, опубликованными 11 ноября 2020 года («Проект рекомендаций»). Они стремятся выполнить требования решения Schrems II Суда Европейского союза в прошлом году и последовать за публикацией в начале этого месяца окончательного исполнительного решения Европейской комиссии по стандартным договорным положениям о передаче персональных данных в третьи страны.

*Ключевые выводы*

Многие из рекомендаций остались неизменными по сравнению с предыдущими проектами рекомендаций, однако есть некоторые заметные различия:

Экспортеры данных должны учитывать, эквивалентна ли защита передаваемых персональных данных той, которая гарантируется в ЕЭЗ, как после передачи персональных данных, так и во время передачи данных от экспортера в страну импортера.

При проведении оценки воздействия передачи («TIA») в Рекомендациях для экспортеров данных делается особый упор на оценку практики, действующей в третьей стране, наряду с соответствующим законодательством, в том числе там, где это законодательство формально соответствует стандартам ЕС. Если существуют несовместимые практики в третьей стране (независимо от правового режима в этой третьей стране), необходимо будет принять дополнительные дополнительные меры.

Если TIA обнаруживает, что соответствующее законодательство в третьей стране может быть «проблематичным», экспортер может продолжить передачу без принятия дополнительных мер, если он считает, что проблемное законодательство не будет применяться на практике к переданным данным и / или импортер. Однако есть много дополнительных препятствий, через которые нужно пройти, чтобы продемонстрировать и задокументировать (в подробном отчете) в сотрудничестве с импортером данных, что закон в третьей стране не интерпретируется и / или не применяется на практике. Рекомендации включают длинный список «возможных источников для оценки третьей страны» в Приложении 3 в порядке предпочтения от золотого стандарта «прецедентное право Суда Европейского Союза» до «внутренние отчеты или записи импортера, прямо указывающие на то, что запросы на доступ не поступали в течение достаточно длительного периода; и предпочтение отдается заявлениям и отчетам, предусматривающим ответственность импортера и / или выпущенным внутренними органами с некоторой автономией, такими как внутренние аудиторы, DPO и т. д.» Главный вывод заключается в том, что планка для документального подтверждения того, что данные вряд ли будут доступны на практике, была установлена чрезвычайно высокой, что добавило к уже существующему значительному количеству дополнительных документов для экспортеров и импортеров.

В отличие от подхода, принятого Европейской комиссией, в проекте рекомендаций было указано, что субъективные факторы, такие как вероятность риска причинения вреда субъекту данных, не должны приниматься во внимание при проведении TIA. Теперь, на первый взгляд, заключительные Рекомендации, похоже, используют более широкий подход, заявляя, что экспортеры данных могут

учитывать «задокументированный практический опыт импортера с соответствующими предыдущими случаями запросов на доступ, полученных от государственных органов в третьей стране», когда проведение TIA. Однако это очевидное приближение к подходу, в большей степени основанному на оценке риска, сопровождается рядом существенных оговорок, в том числе:

Экспортер данных может использовать опыт импортера в качестве дополнительного источника информации только в том случае, если третья страна не препятствует импортеру предоставлять информацию о запросах государственных органов о раскрытии или отсутствии таких запросов. Это, по-видимому, исключает переводы в некоторые страны, например, в США, где информирование третьих сторон о получении запроса о раскрытии информации может рассматриваться как уголовное преступление, связанное с «предупреждением». В самом деле, правонарушение «без предупреждения» не является уникальным для законов США; это характерно для многих режимов перехвата по всему миру.

Соответствующий и документированный опыт импортера должен быть подтвержден и не противоречив…

Отсутствие предыдущих примеров запросов, полученных от импортера не может рассматриваться, сам по себе, как решающий фактор, позволяющий передача продолжить работу без дополнительных мер. Эта информация может рассматриваться только вместе с другими типами информации, полученной как часть общего TIA.

В проекте рекомендаций EDPB принял узкое толкование отступлений в статье 49 GDPR, ограничивая использование отступлений «случайными и неповторяющимися передачами».». В заключительных Рекомендациях EDPB, похоже, принял такой же узкий подход, заявив, что отступления от статьи 49 не могут стать «правилом» на практике, но должны быть ограничены конкретными ситуациями. Тем не менее, полезно, что в заключительных Рекомендациях больше не говорится прямо, что статья 49 должна быть ограничена в использовании «случайными и неповторяющимися передачами». Мы ожидаем, что, несмотря на осторожные указания в окончательных Рекомендациях, статья 49 станет более обычным и популярным механизмом для оправдания переводов, учитывая высокую планку, установленную Рекомендациями, чтобы можно было полагаться на стандартные договорные положения. Эти два варианта не являются взаимоисключающими, и мы также ожидаем, что экспортеры будут стремиться полагаться на Статью 49 «в той мере, в какой» они не могут оправдать передачи на основе другого механизма Главы V. Судебные разбирательства по этим подходам и апелляции в отношении принудительных мер со стороны регулирующих органов, применяющих Рекомендации EDPB, неизбежны, учитывая капризы основного закона.

Рекомендации подтверждают, что дополнительные обязательства, которые, возможно, потребуется включить в BCR в результате решения Schrems II, будут включены в обновленное руководство, в соответствии с которым все группы, полагающиеся на BCR как инструменты передачи, должны будут согласовать свои существующие и будущие BCR.

*Что дальше?*

Важно помнить, что Рекомендации не имеют обязательной юридической силы. Они представляют собой не более чем интерпретацию основного закона, изложенного в самом решении по делу Schrems II и в главе V GDPR, хотя интерпретация специализированных регулирующих органов имеет тенденцию иметь значение в национальных судах государств-членов. Учитывая высокую планку, установленную Рекомендациями для возможности полагаться на стандартные договорные положения, мы ожидаем, что многие экспортеры потерпят неудачу и что принудительные меры, апелляции и судебные разбирательства неизбежны. Потребуется время, чтобы эти апелляции и дела дошли до рассмотрения в судах и чтобы прояснить фактические правовые стандарты оказания помощи. В настоящее время сохраняется большая правовая неопределенность по теме международных переводов.

Хотя Рекомендации содержат указания и подтверждают мнение EDPB о предпочтительном пошаговом подходе, необходимом для выполнения решения Schrems II, требуемый уровень оценки, подробной документации и обоснования, изложенный в Рекомендациях, вероятно, будет сложной задачей для предприятий. В частности, требование рассмотреть практику, действующую в третьей стране, которая может продемонстрировать, что законодательства, соответствующего стандартам ЕС в третьей стране, недостаточно, а также установление того, что «проблемное законодательство» будет очень сложно применить на практике.

Команда глобальной защиты данных, конфиденциальности и безопасности в DLA Piper разработала стандартизированную методологию передачи данных, чтобы помочь клиентам проводить оценку воздействия передачи в соответствии с решением Schrems II и главой V GDPR, полагаясь на SCC или другие механизмы передачи. Для получения дополнительной информации посетите нашу глобальную веб-страницу передачи данных». ***(EDPB adopts final Recommendations on Supplementary Measures // DLA Piper (https://blogs.dlapiper.com/privacymatters/edpb-adopt-final-recommendations-on-supplementary-measures/). 23.06.2021).***

***

**«Большая часть (35%) утечек приходится на фотографирование и скриншоты экрана. Еще в 13% случаев инсайдеры делают физические копии документов. Только 30% утечек происходит через мессенджеры, e-mail и соцсети.**

Такие данные публикует “КоммерсантЪ” со ссылкой на исследование компаний «Крок» и EveryTag, посвященное наиболее популярным каналам утечек данных от инсайдеров из финансового, промышленного сегментов, ритейла и IT.

Передача физических копий документов и фотографирование стали заметными каналами утечек на фоне перехода компаний на удаленную работу, полагают в «Кроке». При этом 76% опрошенных организаций сообщили, что знают об утечках и пытаются расследовать их, 21% компаний говорят, что у них нет возможностей найти инсайдеров, а 17% признались, что даже не отслеживают подобные инциденты.

Также 48% опрошенных уверены, что классические системы защиты от утечек (DLP-системы) не могут оградить конфиденциальные данные от фотографирования и передачи их физических копий.

Так, например, инсайдеры в одной из компаний добывающей отрасли, где была установлена DLP-система, сливали в Telegram-каналах документы, раскрывающие детали сделок по освоению месторождения, рассказали в EveryTag. Обнаружить одного из ключевых инсайдеров удалось путем симуляции утечки, пояснили в компании. В подобных случаях под видом важных разным сотрудникам рассылаются (или предоставляется доступ другим способом) разные сведения, уточнили в «Ростелеком-Соларе». И по тому, какая именно информация утекает, определяется инсайдер. Таким способом в 2008 году воспользовался Илон Маск для поиска источника инсайдерских утечек в Tesla Motors.

Более 30% умышленных утечек по вине персонала совершается с помощью фотографирования экранов на смартфоны или через скриншоты, подтверждает руководитель направления аналитики и спецпроектов ГК InfoWatch Андрей Арсентьев. Такой способ часто применяется в кредитно-финансовых организациях, уточняет руководитель блока защиты от утечек Infosecurity a Softline Company Анна Попова. По ее мнению, рост числа утечек через фото связан с тем, что компании внедряют средства защиты, которые препятствуют обычным способам передачи данных, будь то флешка или пересылка документов, на личную почту с рабочей.

Рост утечек путем фотографирования начали фиксировать еще в 2019 году, когда в финансовом секторе стали активно внедрять DLP, подтверждает гендиректор разработчика DeviceLock DLP Олеся Ярмоленко. По ее словам, полноценной защиты от таких утечек до сих пор нет, но разрабатываются решения, совмещающие DLP-системы и видеонаблюдение.

Некоторые DLP умеют подключаться к фронтальным камерам компьютеров и ноутбуков и анализировать, когда фотографируется экран, говорит Анна Попова. Но систему можно обойти, отключив веб-камеру или спрятав корпус смартфона, признает эксперт.

Топ-менеджер одной из нефтегазовых компаний обнаружил конфиденциальный документ, утекший из компании,– файл сфотографировали на телефон и выложили в интернет, рассказывает заместитель гендиректора CorpSoft24 Михаил Папура. «Чтобы определить, кто из сотрудников стал источником утечки, мы предложили установить программу по скрытой маркировке документов»,– говорит он. Она модифицирует каждую копию документов для каждого пользователя, изменяя интервалы между буквами, словами и строками текста таким образом, что человеческий глаз не может увидеть различий, объяснил господин Папура. По его словам, при обнаружении утечки система просканирует файл и станет ясно, кто из сотрудников его скачивал.

Проблему фотографирования могут решить установка умной системы наблюдения и запрет на использование смартфонов на рабочем месте, полагает руководитель практики информационной безопасности Accenture в России Андрей Тимошенко. По его мнению, вскоре появятся решения, которые будут анализировать все, что попадает в объектив фронтальной камеры, и блокировать

экран, если в зоне видимости будет камера». ***(Большая часть информации утекает в виде фотографий // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5839976-Bolshaya-chast-informacii-utekaet.html). 28.06.2021).***

***

## Кібербезпека Інтернету речей

**«На этой неделе Министерство внутренней безопасности США объявило о новой уязвимости цепочки поставок Интернета вещей, которая серьезно повлияет на устройства Интернета вещей.**

DHS и Nozomi Networks Labs объявили о новой уязвимости, обнаруженной в программном компоненте ThroughTek, который широко используется поставщиками камер видеонаблюдения и смарт-устройств.

Подобные уязвимости цепочки поставок Интернета вещей стали более распространенными.

При таком взломе злоумышленники вмешиваются в процесс разработки программного обеспечения, чтобы внедрить вредоносный компонент, такой как инструмент удаленного доступа, который позволит им закрепиться в целевой организации или отдельном лице.

Действительно, по данным Ресурсного центра по краже личных данных, в первом квартале 2021 года количество атак на цепочки поставок в США выросло на 42%, затронув до 7 миллионов человек. Цепи питания уязвимости могут размножаться быстро, так как код копируется и включены в различные продукты, как указано в «конечных состояний цепи поставок, оценки» отчет 2019 от конечного, в кибербезопасность компании IoT.

«Кибератаки на цепочки поставок представляют собой особую сложность для специалистов по безопасности, поскольку их характер позволяет быстро распространяться этим недостаткам», – сказал Таннер Джонсон, «главный аналитик по безопасности данных, Omdia. «Повсеместность широко используемых аппаратных и программных технологий означает, что, когда такие уязвимости приводят к экспоненциальному увеличению последствий успешной атаки, что делает эти типы недостатков очень востребованными среди потенциальных противников».

Уязвимость цепочки поставок ThroughTek может затронуть миллионы устройств Интернета вещей

Компонент ThroughTek является частью цепочки поставок для многих производителей оригинального оборудования (OEM) камер видеонаблюдения потребительского уровня и устройств IoT. Компания ThroughTek заявляет, что ее технология используется несколькими миллионами устройств, подключенных к Интернету вещей (IoT).

Пакет разработки программного обеспечения (SDK) ThroughTek P2P обеспечивает удаленный доступ к аудио / видео потокам через Интернет.

Несколько миллионов подключенных устройств, включая IP-камеры, камеры для наблюдения за ребенком, а также роботизированные и аккумуляторные устройства. P2P позволяет клиенту получать доступ к аудио / видео потокам через Интернет. Новая уязвимость, обнаруженная в часто используемом программном компоненте, обнаруженном в камерах видеонаблюдения и интеллектуальных датчиках, позволяет неавторизованным зрителям получить доступ к видеопотокам и посягнуть на жизнь потребителей. А для бизнес-пользователей – доступ к конфиденциальной информации о бизнесе, производстве, сотрудниках и клиентах.

Эта уязвимость возникает вслед за другими громкими нарушениями, включая утечки данных SolwarWinds и Blackbaud, которые сигнализируют о тревожном росте уязвимостей в цепочке поставок.

По мере роста уязвимостей цепочки поставок предприятиям необходимо остерегаться возможных нарушений и тщательно анализировать код, который они включают в свой ИТ-ландшафт.

«Уязвимости цепочки поставок, нацеленные на устройства IoT, добавляют сложности, которые усугубляются огромным количеством уязвимых подключенных устройств на местах: примерно 40 миллиардов к концу 2020 года», – сказал Джонсон. «Защита устройств Интернета вещей может быть более сложной задачей, чем традиционные сетевые компоненты, поскольку многие из этих устройств не имеют базовых функций, таких как операционные системы, пользовательские интерфейсы или встроенные агенты, с которыми можно было бы взаимодействовать. В результате организация может совершенно не осознавать, что успешная атака на цепочку поставок скомпрометировала компоненты Интернета вещей.

*Защита от уязвимости цепочки поставок Интернета вещей*

CISA рекомендует пользователям принять меры для минимизации риска использования этой уязвимости, включая рассмотрение следующих действий:

Следуйте рекомендациям по сертификации Агентства по кибербезопасности и безопасности инфраструктуры для исправления ситуации.

Дальнейшие соображения включают оценку политики безопасности и конфиденциальности поставщика камеры и юрисдикции, в которой находится поставщик.

Nozomi Networks рекомендует, чтобы пользователи промышленной и критически важной инфраструктуры включали P2P только в тех редких случаях, когда поставщик устройства может предоставить подробное техническое объяснение того, почему алгоритмы, используемые в их продуктах, являются безопасными.

Свести к минимуму уязвимость сети для всех устройств и / или систем системы управления и убедиться, что они недоступны из Интернета.

Обнаруживайте сети систем управления и удаленные устройства за межсетевыми экранами и изолируйте их от бизнес-сетей.

Когда требуется удаленный доступ, используйте безопасные методы, такие как виртуальные частные сети, распознавание VPN может иметь уязвимости и должно быть обновлено до самой последней доступной версии. Также знайте, что безопасность VPN зависит от уровня безопасности подключенных к нему

устройств». ***(Lauren Horwitz. New ThroughTek IoT Supply Chain Vulnerability Announced // Informa PLC (https://www.iotworldtoday.com/2021/06/16/new-throughtek-iot-supply-chain-vulnerability-announced/). 16.06.2021).***

***

## Кіберзлочинність та кібертерроризм

**«Были сформированы новые словарные слова для описания онлайн-мошенничества. Фишинг, о котором сейчас все знают, – это когда мошенник использует предлог в электронном письме, чтобы заставить кого-то щелкнуть ссылку или вложение в письме для развертывания вредоносных программ и программ-вымогателей.**

Социальная инженерия – это когда преступники проводят онлайн-поиск людей и компаний, просматривая профили Facebook и LinkedIn и используя поиск в Google, чтобы узнать как можно больше о компании и ее сотрудниках и разработать досье на компанию для запуска фишинга, вишинга или обманывающая афера.

Вишинг может произойти, например, когда преступник покупает домен, аналогичный домену компании, затем добавляет некоторые условия безопасности, чтобы они выглядели так, как будто они принадлежат ИТ-отделу компании, и звонит сотруднику, рассказывает ему историю о том, как они необходимо обновить VPN или добавить дополнительные меры безопасности, отправляет сотруднику электронное письмо с поддельного адреса электронной почты компании и, пока он разговаривает с сотрудником по телефону, убеждает сотрудника ввести свое имя пользователя и пароль во всплывающее окно, сейчас предоставление преступнику полного доступа к аккаунту сотрудника.

И smishing (это настолько ново, что проверка орфографии не распознает его) – это когда мошенники используют текст (SMS-сообщения) в качестве уловки вместо электронной почты или телефонного звонка.

Люди склонны доверять текстовым сообщениям больше, чем электронным письмам. Они также читают их чаще и быстрее, чем электронные письма. Мошенники используют старые методы с новыми технологиями, чтобы заставить людей переходить по встроенным ссылкам, чтобы внедрить вредоносное ПО в телефоны людей или отказаться от личных или корпоративных учетных данных. Теперь мошенничество использует текстовые сообщения.

Это должно вызывать беспокойство у ИТ-специалистов, поскольку очень многие сотрудники используют свои личные телефоны для работы. Несмотря на то, что сотрудники становятся жертвами атак на их личные телефоны, мошеннические мошенничества могут представлять угрозу для корпоративной безопасности. ИТ-специалисты могут пожелать добавить умение в качестве метода при обучении сотрудников безопасности, чтобы они знали о новейших методах, используемых преступниками». ***(Linn Foster Freedman. Phishing, Vishing, and Smishing-Your Employees Need to Know the Newest Schemes // Robinson & Cole LLP***

***(https://www.dataprivacyandsecurityinsider.com/2021/06/phishing-vishing-and-smishing-your-employees-need-to-know-the-newest-schemes/). 24.06.2021).***

***

**«Колледж штата Айова отменил все занятия на четыре дня после того, как хакеры вынудили его отключить части школьной сети и телефонной системы.**

Взлом, который выглядит как программа-вымогатель, вынудил Общественный колледж Де-Мойна (DMACC) прибегнуть к публикации обновлений на Facebook, Twitter и в базовой версии своего сайта. Школа также попросила преподавателей, сотрудников и студентов избегать использования Microsoft Office 365, а также популярной платформы онлайн-обучения Blackboard.

В четверг, 3 июня, DMACC объявила, что «в настоящее время работает над восстановлением Интернет-услуг в колледже» и что занятия в этот день были отменены. Затем колледж отменил все занятия в пятницу, а также в понедельник и вторник на этой неделе, согласно его официальной странице в Facebook.

В среду колледж попросил некоторых студентов приехать в кампус для очных занятий.

«Уроки DMACC, которые включают в себя любой личный компонент (либо полностью, либо частично), будут возобновлены и будут проводиться в обычное время и по расписанию», – объявил DMACC на своем официальном веб-сайте, который теперь включает только обновления о кибератака и ее последствия для школьной деятельности. «Для наших студентов и преподавателей это означает, что если какая-либо часть вашего класса обычно встречается лично, эта часть урока возобновится в соответствии с графиком, начиная со среды, 9 июня».

По состоянию на среду онлайн-уроки все еще отменены и возобновятся только «через 24 часа после восстановления сети», как написала школа на своем сайте.

«У нас есть доступ к заданиям, но у нас нет доступа к материалам, поэтому вы в основном делаете это вслепую. Вы просто предполагаете», – сказала We Are Iowa студентка второго семестра Бренна Вобл.

Школа находится в середине летнего семестра, где есть как онлайн-классы, так и очные, в то время как «администраторы DMACC планируют начать «новую норму» в работе колледжа, когда осенние занятия возобновятся 25 августа», – говорится в сообщении. кешированная версия страницы веб-сайта школы об обновлениях COVID-19.

В начале пандемии прошлого года DMACC закрыл и отменил очные занятия. Прошлым летом DMACC объявил, что в осеннем семестре 2020 года будет предлагать как личные, так и онлайн-классы.

DMACC не публиковал подробностей кибератаки, только заявив в Facebook, что она «потребовала от нас отключить части нашей сети».

Роб Денсон, президент школы, сказал в сообщении, размещенном на сайте, что ИТ-отдел работает с «внешними кибер-экспертами», чтобы восстановить обслуживание и «определить, какие данные были скомпрометированы». Денсон добавил, что к расследованию подключилось ФБР.

«На сегодняшний день у нас нет доказательств того, что какая-либо информация о студентах или преподавателях была получена или находится под угрозой в результате этого инцидента», – написал он.

На данный момент неясно, является ли это атакой программы-вымогателя и какая хакерская группа стояла за ней…». ***(Lorenzo Franceschi-Bicchierai. Hackers Force Iowa College to Cancel Classes for Four Days // VICE MEDIA GROUP (https://www.vice.com/en/article/3aqaa8/hackers-force-iowa-college-to-cancel-classes-for-four-days). 09.06.2021).***

***

**«Akamai подтвердила, что отказ одного из ее DDoS-сервисов Prolexic был виновен в отключении онлайн-сервисов некоторых крупных банков и систем авиакомпаний Австралии в четверг днем.**

Компания заверила, что проблема не была вызвана обновлением системы или кибератакой, и уточнила, что значение таблицы маршрутизации, используемое ее службами Prolexic DDoS, было «непреднамеренно превышено».

«Результатом стало непредвиденное прерывание обслуживания», – заявили в компании.

Поставщик услуг из США, который позиционирует себя как «крупнейшая и самая сложная периферийная платформа в мире», заявил, что обнаружил проблему немедленно, и пострадавшие клиенты были предупреждены в течение нескольких секунд. Проблемы начали появляться примерно в 14:20 AEST в четверг.

«Воздействие было ограничено клиентами Akamai, использующими версию 3.0 сервиса Routed», – подтвердила компания в своем сообщении.

«Многие из примерно 500 клиентов, использующих эту услугу, были автоматически перенаправлены, что позволило восстановить работу в течение нескольких минут. Подавляющее большинство оставшихся клиентов изменили маршрут вручную вскоре после этого».

Пострадавшие клиенты включали три из четырех крупных австралийских банков – Commonwealth Bank of Australia, Westpac и ANZ, а также Australia Post и Virgin Australia. Каждый из них отправился в Twitter, чтобы сообщить клиентам о проблеме.

«Нам известно, что некоторые из вас испытывают трудности с доступом к нашим услугам, и мы срочно расследуем их. Приносим извинения и благодарим за терпение, мы скоро предоставим обновленную информацию», – сказал CBA. Аналогичные замечания сделали Westpac и ANZ.

Virgin Australia написала в Твиттере, что отключение повлияло на ее веб-сайт и контакт-центр. Между тем, Australia Post сообщила, что это произошло из-за «внешнего» отключения.

Сервис был восстановлен к 18:47 AEST.

С тех пор Akamai принесла извинения своим клиентам и затронула конечных пользователей.

«Мы предприняли шаги, чтобы предотвратить повторение этой проблемы. Мы также будем работать над тем, чтобы каждый клиент Akamai был настроен на автоматическое изменение маршрута в будущем», – заявили в компании». ***(Aimee***

***Chanthadavong. Akamai apologises after outage left Australia's major banks and airline systems offline // ZDNet (https://www.zdnet.com/article/akamai-apologises-after-outage-left-australias-major-banks-and-airline-systems-offline/). 17.06.2021).***

***

**«Согласно новым данным по ЕС, полученным CNN, за последний год количество кибератак против критических целей в Европе удвоилось, поскольку пандемия вытеснила жизни в помещениях и в Интернете.**

Агентство Европейского Союза по кибербезопасности, ENISA, сообщило CNN, что в 2020 году было совершено 304 серьезных вредоносных атаки на «критические сектора», что более чем вдвое превышает 146, зарегистрированных годом ранее.

Агентство также сообщило о 47% -ном росте атак на больницы и медицинские сети за тот же период, поскольку те же преступные сети пытались нажиться на наиболее важных услугах, связанных с пандемией.

Цифры показывают растущее глобальное влияние кибератак, часто в форме программ-вымогателей, которые недавно вызвали хаос в Соединенных Штатах, когда группа Darkside нацелена на сеть Colonial Pipeline, вызывая очереди на заправках из-за опасений нехватки.

Пандемия означала, что «множество услуг было предоставлено онлайн, и это произошло в спешке, поэтому о безопасности позаботились второстепенно», – сказал Апостолос Малатрас, руководитель группы знаний и информации в ENISA. В то же время люди не выходили из дома и у них было время исследовать уязвимости в системах и критической инфраструктуре, добавил он.

Исследования предприятий, проведенные британской фирмой по обеспечению безопасности Sophos, также показали, что средняя стоимость атаки с использованием программ-вымогателей за год удвоилась. Опрос оценил затраты на 2020 год в 761 106 долларов, но к этому году эта цифра подскочила до 1,85 миллиона долларов. В стоимость входит страховка, потеря бизнеса, очистка и любые платежи от программ-вымогателей.

Рост стоимости отражает большую сложность некоторых атак, сказал Джон Шиер, старший советник по безопасности в Sophos, добавив, что, хотя количество атак снизилось, их изощренность возросла.

«Похоже, они пытаются быть более целеустремленными», – сказал Шиер. «Таким образом, они взламывают компании, точно понимая, какую компанию они взломали, и пытаются проникнуть как можно более полно, чтобы затем извлечь как можно больше денег».

*Новые угрозы*

И Шайер, и Малатрас указали на последнюю угрозу «тройного вымогательства», когда злоумышленники блокируют данные в системах цели с помощью шифрования и извлекают их, чтобы они могли угрожать опубликовать их в Интернете. По их словам, злоумышленники затем переходят к третьему этапу, используя эти данные для атаки на системы цели и шантажа ее клиентов или контактов.

«Если вы являетесь клиентом этой компании, данные которой были украдены, они будут угрожать раскрыть вашу информацию или также позвонят в другие компании, которые являются вашими партнерами», – сказал Шиер. Он добавил, что самый высокий выкуп, о котором он слышал, составил 50 миллионов долларов.

Еще одна угроза связана с «бесфайловыми атаками», при которых программа-вымогатель не содержится в файле, доступ к которому обычно осуществляется в результате человеческой ошибки, например при нажатии на подозрительную ссылку или открытии вложения. Бесфайловые атаки проникают в операционную систему компьютера и часто хранятся в его оперативной памяти, что затрудняет их обнаружение антивирусным программным обеспечением.

На прошлой неделе Министерство юстиции США объявило о планах координировать свои усилия по борьбе с программами-вымогателями с использованием тех же протоколов, что и для терроризма, а администрация Байдена рассматривает возможность наступления на основные группы программ-вымогателей и киберпреступников.

Такой подход будет соответствовать подходу других союзников, включая Великобританию, которая в ноябре публично признала существование Национальной киберсилы (NCF) для борьбы с ключевыми угрозами для Великобритании в Интернете. Представитель GCHQ, британской организации по разведке и информационной безопасности, сказал CNN: «В прошлом году мы признали NCF, партнерство между GCHQ и Министерством обороны, с полномочиями пресекать противников... используя кибероперации для пресечения враждебных действий. государственная деятельность, террористы и криминальные сети, угрожающие безопасности Великобритании».

*Отслеживание преступных операций*

Хотя эксперты в области правопорядка и безопасности говорят, что лучше всего не платить выкуп, поскольку это поощряет преступников, у компаний, которые платят, есть некоторая надежда.

Более совершенные технологии позволяют некоторым охранным фирмам отслеживать криптовалюту, обычно биткойн, когда преступники перемещают ее между разными учетными записями и криптовалютами.

На этой неделе следователям ФБР удалось вернуть часть денег, выплаченных группе вымогателей Darkside сетью Colonial Pipeline после атаки, которая привела к значительным перебоям в поставках газа в США.

Фирма кибербезопасности Elliptic, которая помогает ФБР в таких следах, заявила, что то короткое время, когда у Darkside были деньги, означало, что она не могла адекватно отмыть деньги в киберпространстве, поэтому маршрут было легко обнаружить.

«В настоящий момент преступники хотят обналичить деньги в евро или чем-то еще, чтобы извлечь выгоду из своей преступной деятельности», – сказал Том Робинсон, главный научный сотрудник Elliptic. Это означает, что криптовалюта обычно отправляется на финансовую биржу в реальном мире, чтобы превратить ее в реальные деньги, сказал он.

«Если биржа регулируется, то вы должны идентифицировать их клиентов и сообщать о любой подозрительной активности», – сказал Робинсон.

По его словам, уловки, используемые преступными группировками для сокрытия маршрута незаконной криптовалюты, становятся все сложнее. Некоторые используют «микшерные кошельки», которые позволяют смешивать криптовалюты пользователей, например, перетасовывать использованные банкноты, что затрудняет отслеживание владения. Робинсон сказал, что регулирование этих кошельков и всех обменов поможет снизить криминальные стимулы к использованию программ-вымогателей.

«Речь идет о выявлении преступников, а также о том, чтобы этим преступникам было очень трудно обналичить деньги», – сказал Робинсон. «Это означает, что у нас меньше стимулов для совершения такого рода преступлений». ***(Nick Paton Walsh. Serious cyberattacks in Europe doubled in the past year, new figures reveal, as criminals exploited the pandemic // Cable News Network (https://edition.cnn.com/2021/06/10/tech/europe-cyberattacks-ransomware-cmd-intl/index.html). 10.06.2021).***

***

**«В новом отчете Auth0 было обнаружено, что правительственные учреждения, а также туристические и розничные компании продолжают сталкиваться с чрезмерным количеством атак по подбору учетных данных.**

Auth0, который недавно был приобретен Okta за 6,5 миллиардов долларов, опубликовал потрясающую статистику того, что они видят в своем отчете о состоянии безопасной идентификации.

За первые три месяца 2021 года Auth0 обнаружил, что на заполнение учетных данных приходилось 16,5% попыток входа в систему на его платформе, с пиком более 40% ближе к концу марта.

По данным Auth0, около 15% всех попыток зарегистрировать новую учетную запись могут быть связаны с ботами.

В отчете также говорится, что Auth0 поддерживает постоянно растущую базу данных пар имя-пароль, которые, как известно, были скомпрометированы в результате утечки данных. В течение первых 90 дней 2021 года платформа Auth0 обнаруживала в среднем более 26 600 взломанных паролей, используемых каждый день. 9 февраля это число достигло максимума на 2021 год – более 182000.

Согласно отчету, злоумышленники потратят от 50 до 1000 долларов на подтвержденные учетные данные из записей кредитных карт, криптографических учетных записей, учетных записей социальных сетей и даже учетных записей Netflix.

Наиболее часто обнаруживаемые угрозы на платформе Auth0 включают заполнение учетных данных, мошеннические регистрации, обход MFA и использование взломанного пароля.

Платформа Auth0 обнаружила, что 39% IP-адресов, связанных с атаками с заполнением учетных данных, находятся в США. На сферу технологий и туризма приходится более 50% всех атак с использованием SQL-инъекций, наблюдаемых на платформе.

Туристические предприятия и предприятия розничной торговли чаще всего подвергаются грубым атакам, за ними следуют государственные учреждения, компании, предоставляющие промышленные услуги, и технологические организации. Отрасль технологий сталкивается с наибольшим количеством попыток грубой силы MFA – 42% на платформе Auth0, затем идут потребительские товары с 15% и финансовые услуги с 13%.

Auth0 отметил, что злоумышленники часто нацелены на программы вознаграждения, предлагаемые ресторанами или магазинами, потому что «они редко надежно защищены, а выгоды легко монетизировать».

Согласно отчету, компании в сфере финансовых услуг лидируют по внедрению МИД, за ними следуют технологии и промышленные услуги. Хотя большинство людей выбирают электронную почту или SMS в качестве фактора MFA, многие также используют одноразовые коды доступа на основе времени.

Многие организации в сфере технологий, финансовых услуг и промышленных услуг также используют программы обнаружения ботов как способ замедлить или ограничить атаки с заполнением учетных данных.

Дункан Годфри, вице-президент по безопасности в Auth0, сказал, что компаниям, занимающимся безопасностью, становится все сложнее и сложнее защитить личность своих клиентов из-за повсеместной неспособности защитить данные и распространенности взломанных паролей.

Годфри объяснил, что доступность автоматизированных средств атаки превратила скромный пароль в «защитную меру из прошлого».

Множественные взломы и кибератаки за последний месяц были вызваны повторным использованием паролей или данных учетной записи, которые были утекли в ходе предыдущих атак». ***(Jonathan Greig. Travel and retail industries facing wave of credential stuffing attacks // ZDNet (https://www.zdnet.com/article/travel-and-retail-industries-facing-wave-of-credential-stuffing-attacks/). 16.06.2021).***

***

**«Nokia Deepfield обнаружила 100%-ное увеличение ежедневного пикового трафика DDoS в период с января 2020 года по май 2021 года.**

Подразделение Nokia по анализу IP-сетей и данных смогло провести анализ отпечатков пальцев и происхождения сетевого трафика благодаря работе с глобальными поставщиками услуг, компаниями веб-масштаба и цифровыми предприятиями.

Крейг Лабовиц, технический директор Nokia Deepfield, на этой неделе на NANOG82 представил результаты глобального анализа DDoS-трафика.

Анализ показал, что наблюдается значительный рост объемных DDoS-атак с высокой пропускной способностью, большинство из которых исходят всего от нескольких десятков хостинговых компаний.

Лабовиц сказал ZDNet, что общепринятое мнение гласит, что DDoS-атаки происходят со всего Интернета и что DDoS-атаки невозможно заблокировать у источника.

«Но общепринятое мнение неверно. Мы можем остановить подавляющее большинство DDoS-атак внутри этих 50 компаний (например, если хостинговые

компании блокируют плохих клиентов) или с помощью действий, предпринятых 10-15 поставщиками интернет-услуг, которые подключают эти хостинговые компании к Интернету,» он сказал.

Исследователи также обнаружили доказательства DDoS-атак с потенциальной угрозой «более 10 Тбит / с, что до пяти раз выше, чем у крупнейших известных текущих атак». По словам Лабовица, самая крупная зарегистрированная DDoS-атака составила около 2 Тбит / с. В октябре Google заявил, что в 2017 году он имел дело с атакой со скоростью 2,54 Тбит / с, запущенной спонсируемой государством группой из Китая, что стало крупнейшей атакой, о которой сообщалось ранее.

По данным Nokia Deepfield, масштабы атак увеличивались отчасти из-за «растущего числа открытых и небезопасных интернет-сервисов и устройств IoT». Например, всего шесть недель назад в результате DDoS-атаки было уничтожено 200 государственных и университетских веб-сайтов по всей Бельгии.

Лабовиц добавил, что кривая роста DDoS-атак носит экспоненциальный характер из-за взрывного роста IoT и Cloud, которые резко увеличивают количество серверов и устройств, которые могут быть задействованы в DDoS-атаках.

«Вторым важным моментом моей сегодняшней презентации является то, что экспоненциальная кривая роста DDoS-атак представляет реальную угрозу для Интернета. Это связано с увеличением количества серверов (которые могут быть использованы для запуска DDoS-атак) и большого количества IoT-устройств с нестандартная безопасность или безопасность по умолчанию (следовательно, открытая для взлома и контроля ботнетов)», – сказал Лабовиц.

«Я считаю, что это просто чистая удача, ошибки в атаках и т. Д. В том, почему зарегистрированные DDoS-атаки значительно ниже 10+ Тбит / с (и, возможно, намного больше) потенциала DDoS-атак».

Компания также обнаружила, что за последние 15 месяцев расширилось количество DDoS-атак для услуг по найму, доступных для атак, стремящихся нанести значительный ущерб индивидуальным и крупномасштабным связям и доступности услуг.

В течение 2020 года, когда сообщества по всему миру ввели блокировку в рамках усилий по сдерживанию COVID-19, Nokia Deepfield сообщила, что трафик DDoS увеличился на 50%.

«Продолжающийся рост интенсивности, частоты и изощренности DDoS-атак привел к 100% -ному увеличению «высокого уровня водяного знака» суточных пиков DDoS-атак – с 1,5 Тбит / с (январь 2020 г.) до более 3 Тбит / с (май 2021 г.)» компания сказала.

Для каждого участника экосистемы сетевой безопасности – конечных пользователей, поставщиков, поставщиков услуг, разработчиков облачных вычислений, регулирующих органов и правительств – важно понимать опасность, которую DDoS представляет для доступности интернет-контента, приложений и критически важных сервисов подключения, Лабовиц добавлен». ***(Jonathan Greig. 100% increase in daily DDoS traffic in 2020 as potential grows for 10 Tbps attack:***

***Nokia // ZDNet (https://www.zdnet.com/article/100-increase-in-daily-ddos-traffic-in-2020-as-potential-grows-for-10-tbps-attack-nokia/). 15.06.2021).***

***

**«Игровой гигант Electronic Arts был взломан, и теперь кибератаки продают доступ к играм и серверам компании, согласно скриншотам подпольных хакерских форумов, полученным Motherboard.**

Сообщения, найденные на хакерских форумах, указывают на то, что злоумышленники взяли у компании 780 ГБ данных и имеют полный доступ к серверам подбора игроков FIFA 21, ключам API FIFA 22 и некоторым программным средствам разработки для Microsoft Xbox и Sony. Они также претендуют на то, чтобы иметь гораздо больше, включая исходный код и инструменты отладки для Frostbite, который используется в самых популярных играх EA, таких как Battlefield, FIFA и Madden.

«У вас есть полная возможность использовать все сервисы EA», – говорится в сообщении одного злоумышленника, отмечая, что во всем мире зарегистрированы сотни миллионов пользователей EA и почти девять миллионов пользователей FIFA. Сообщения включали образцы того, что было украдено, и свидетельствовали о том, что злоумышленники продают пакет данных и доступ за 28 миллионов долларов.

В заявлении для ZDNet представитель EA заявил, что это не атака с использованием программ-вымогателей, и заявил, что «во время атаки было украдено ограниченное количество исходного кода игры и связанных инструментов». Компания заявила, что не ожидает какого-либо влияния на ее игры или бизнес.

«К данным игроков не было доступа, и у нас нет оснований полагать, что существует какой-либо риск для конфиденциальности игроков», – сказал представитель EA. «Мы активно работаем с представителями правоохранительных органов и другими экспертами в рамках текущего уголовного расследования».

Группа кибер-исследований и разведки BlackBerry поделилась с ZDNet снимками экрана с заметками кого-то, кто стоит за атакой.

Эрик Милам, вице-президент по исследованиям и аналитике BlackBerry, сказал, что EA, вероятно, стала мишенью, потому что «сказать, что вы взломали EA, все равно что сказать, что вы взломали Blizzard». Имея исходный код нескольких видеоигр, злоумышленники могут скомпилировать и продать игру до того, как она выйдет, а также добавить свои собственные бэкдоры в определенные игры. Что-то вроде этого «дало бы им доступ к большому количеству компьютеров».

«Исходный код позволяет анализировать все, что там есть, без необходимости реконструировать. Исходный код также может помочь им понять тип безопасности при обмене информацией и платежами», – сказал Милам. «Исходный код может содержать жестко запрограммированные учетные данные, ключи и т. Д., Которые можно использовать в другом месте или разрешить дополнительные возможности удаленного кода».

EA – далеко не первая игровая компания, которую взломали: и Capcom, и CD Projekt пострадали от атак в прошлом году. CD Projekt сообщила об атаке

программы-вымогателя в феврале, а Capcom объявила о взломе в ноябре, который теперь имеет далеко идущие правовые последствия для компании.

Сама EA была взломана в 2011 году, и ей пришлось столкнуться с рядом уязвимостей, обнаруженных в 2019 году.

Раджив Пимпласкар, директор по рискам компании Veridium, занимающейся кибербезопасностью, сказал, что, как и у Capcom, может быть несколько последующих последствий, таких как потеря учетных данных клиентов, биографических данных и т. Д., Помимо потерь интеллектуальной собственности.

«EA зарабатывает более 2,7 миллиарда долларов на микротранзакциях или внутриигровых покупках. Сегодня разработчики приложений несут более высокую ответственность за защиту потребителей, и им необходимо все чаще включать меры цифровой идентификации, аутентификации и конфиденциальности на уровне кода для улучшения киберзащиты и смягчения последствий таких форм. воровства», – добавил Пимпласкар.

Эрих Крон, защитник осведомленности в области безопасности в KnowBe4, сказал ZDNet, что было странно, что злоумышленники не пытались выкупить данные у EA, прежде чем продать их на открытом рынке. Он отметил, что служебная информация, обнаруженная в утечке, может быть ценна для конкурентов или может включать информацию или уязвимости, которые могут быть использованы в будущих атаках на продукты EA или клиентов с установленными играми EA.

Многие эксперты добавили, что кража исходного кода игры нанесла особый ущерб такой компании, как EA, у которой есть такие популярные бренды, как FIFA, Madden, Battlefield, Star Wars: Jedi Fallen Order, The Sims и Titanfall.

«Исходный код игры – это проприетарная и конфиденциальная интеллектуальная собственность, которая является стержнем службы или предложения компании. Раскрытие этих данных – все равно что фактически лишить ее жизни», – сказал Сарью Найяр, генеральный директор Gurucul.

«Сердцебиение было прервано, и неизвестно, как эта атака в конечном итоге повлияет на жизнь игровых сервисов компании в будущем». ***(Jonathan Greig. Hackers selling access to FIFA matchmaking servers and other games after EA attack // ZDNet (https://www.zdnet.com/article/hackers-selling-access-to-fifa-matchmaking-servers-and-other-games-after-ea-attack/). 10.06.2021).***

***

**«Как стало известно Motherboard, группа хакеров, укравших огромное количество данных у гиганта-издателя игр Electronic Arts, ворвалась в компанию отчасти, обманув сотрудника через Slack и предоставив ему токен входа.**

Группа украла исходный код FIFA 21 и связанных инструментов подбора игроков, а также исходный код движка Frostbite, который используется в таких играх, как Battlefield, и других внутренних инструментах разработки игр. В целом хакеры заявляют, что у них есть 780 ГБ данных, и рекламируют их для продажи на различных подпольных форумах. EA ранее подтвердила данные, затронутые взломом материнской платы.

Представитель хакеров сообщил Motherboard в онлайн-чате, что процесс начался с покупки украденных файлов cookie, продаваемых в Интернете за 10 долларов США, и их использования для получения доступа к каналу Slack, используемому EA. Файлы cookie могут сохранять данные для входа в систему конкретных пользователей и потенциально позволяют хакерам входить в службы от имени этого человека. В этом случае хакеры смогли проникнуть в Slack EA с помощью украденного файла cookie. (Хотя это и не обязательно, но в феврале 2020 года Motherboard сообщила, что группа исследователей обнаружила, что бывший инженер оставил список названий каналов EA Slack в общедоступном репозитории кода).

«Оказавшись в чате, мы отправили сообщение сотрудникам службы поддержки ИТ и объяснили им, что потеряли телефон на вечеринке вчера вечером», – сказал представитель.

Затем хакеры запросили токен многофакторной аутентификации у ИТ-поддержки EA, чтобы получить доступ к корпоративной сети EA. Представитель сказал, что это было успешным два раза.

Попав в сеть EA, хакеры нашли для разработчиков EA сервис для компиляции игр. Они успешно вошли в систему и создали виртуальную машину, дающую им больше информации о сети, а затем получили доступ к еще одной службе и загрузили исходный код игры.

Представитель хакеров предоставил снимки экрана, чтобы подтвердить различные этапы взлома, включая сами чаты Slack. Затем EA подтвердила для Motherboard контуры описания взлома, данные хакерами.

В своем более раннем заявлении EA сообщила: «Мы расследуем недавний инцидент вторжения в нашу сеть, когда было украдено ограниченное количество исходного кода игры и связанных инструментов. Не было доступа к данным игроков, и у нас нет оснований полагать, что они есть. риск для конфиденциальности игроков. После инцидента мы уже внесли улучшения в систему безопасности и не ожидаем, что это повлияет на наши игры или наш бизнес. Мы активно работаем с представителями правоохранительных органов и другими экспертами в рамках этого продолжающегося уголовного расследования».

Представитель хакеров также предоставил Motherboard ряд документов, которые, по их словам, были украдены в ходе взлома. Они включают в себя подборку материалов о PlayStation VR, о том, как EA создает цифровые толпы в играх FIFA, а также документы об искусственном интеллекте в играх…». ***(Joseph Cox. How Hackers Used Slack to Break into EA Games // VICE MEDIA GROUP (https://www.vice.com/en/article/7kvkqb/how-ea-games-was-hacked-slack). 11 04.2021).***

***

**«Согласно новому исследованию, группы безопасности существуют менее чем в трети бразильских организаций, хотя большинство предприятий часто подвергаются кибератакам.**

Согласно опросу, проведенному Instituto Datafolha по заказу Mastercard, около 57% предприятий из секторов образования, финансовых услуг, страхования,

технологий и телекоммуникаций, здравоохранения и розничной торговли часто становятся объектами нападений киберпреступников.

С другой стороны, исследование показало, что только 32% опрошенных организаций имеют специальные группы по кибербезопасности. Хотя 80% респондентов заявили, что вопросы цифровой безопасности важны для них и у большинства есть какой-то план борьбы с потенциальными кибератаками, это не входит в число бюджетных приоритетов для 39% опрошенных.

Среди проанализированных в исследовании сегментов финансовые услуги, страхование, технологии и телекоммуникации являются одними из наиболее подготовленных с точки зрения готовности к кибербезопасности. И наоборот, секторы образования и здравоохранения являются наиболее уязвимыми.

Согласно опросу, наиболее уязвимыми для хакерских атак областями являются финансовый отдел и клиентские базы данных. Опрос Mastercard / Datafolha опросил 351 человека, принимающего решения, в Бразилии в феврале 2021 года.

Опрос перекликается с выводами отдельного исследования восприятия рисков кибербезопасности в Латинской Америке с начала кризиса COVID-19, проведенного консалтинговой фирмой Marsh от имени Microsoft.

Большинство бразильских компаний не увеличили свои инвестиции в информационную и кибербезопасность с момента возникновения пандемии, несмотря на рост угроз, отмечается в исследовании, добавляя, что большинство бразильских компаний вкладывают 10% или меньше своего ИТ-бюджета в эту область». ***(Angelica Mari. Most Brazilian companies lack cybersecurity teams // ZDNet (https://www.zdnet.com/article/most-brazilian-companies-lack-cybersecurity-teams/). 04.06.2021).***

***

**«Переход к работе на дому (WFH) за последний год вызвал историческое изменение в том, как корпорации ведут бизнес.** Это также вызвало серьезные изменения в подходе все более продвинутых злоумышленников, стремящихся воспользоваться этим сдвигом в WFH. Многие злоумышленники теперь пользуются преимуществами новых уязвимостей и очень легко и очень быстро превращают их в вооруженные атаки, в то время как крайние противники теперь сосредоточены на цепочке поставок и целевых атаках. Такое сочетание создает очень сложную среду для любого современного предприятия.

Эти все более сложные угрозы делятся на две категории. Те, которые (1) известны и их легче всего реализовать в целом и (2) хорошо финансируются и планируются, а также являются наиболее сложными и разрушительными. В первом случае есть известные угрозы и уклончивые вредоносные программы. Атаки нулевого дня по-прежнему делятся на две категории, но с растущей вероятностью, что новый нулевой день будет широко использоваться очень быстро. Между тем, к наиболее сложной и опасной категории относятся цепочки поставок и целевые атаки.

Как видно из названия, атака нулевого дня происходит в тот же день, когда обнаруживается новая уязвимость, до того, как доступно исправление. Очевидно,

что, поскольку программный дефект является совершенно новым, стандартные подходы оставляют промежуток между раскрытием нулевого дня и реализацией защиты или исправления, которые злоумышленники могут использовать.

Не менее отвратительны бесфайловые и целевые атаки. Бесфайловая атака – это тип, при котором вредоносное ПО не устанавливается на компьютер, поэтому традиционные антивирусные инструменты, скорее всего, пропустят ее. Что касается целевой атаки, эти конкретные злоумышленники – со значительной смекалкой и ресурсами – преследуют, отслеживают и компрометируют инфраструктуру целевого объекта или, в последнее время, цепочку поставок, чтобы обеспечить доступ многим другим предприятиям. Помимо изощренности, эти злоумышленники как можно дольше сохраняют скрытность в сетях, на которые они нацелены.

Эти угрозы продолжают усложняться. Более того, уязвимости растут. Обе динамики приводят к большей уязвимости к нарушениям.

Что затрудняет предотвращение известных угроз? По правде говоря, традиционные решения безопасности просто не раскрывают основы, что ложится бременем на группы безопасности, которые не имеют надлежащих ресурсов для выявления или исправления уязвимостей, чтобы уверенно избежать утечки данных.

Давайте посмотрим на традиционные подходы к сетевой безопасности, существующие в отрасли. Они имеют ограниченную видимость, то есть трафик часто проверяется только на определенных портах без понимания контекста трафика. Это самая большая проблема. Еще одна проблема – низкая производительность. Хотя добавление однофункциональных устройств в защитный стек может облегчить определенные проблемы, на самом деле включение всех функций безопасности для многих элементов управления безопасностью на сетевом уровне может серьезно повлиять на пропускную способность, что приведет к снижению производительности.

Это еще больше усугубляется тем, что традиционные системы предотвращения или обнаружения вторжений (IPS / IDS) по-прежнему используют те же стратегии защиты, что и до развития ландшафта угроз.

*Необходимость комплексного предотвращения угроз*

Что такое комплексное предотвращение угроз? Короче говоря, это означает, что у вас есть полная видимость и возможность обнаруживать неизвестные угрозы и быстро превращать их в известные угрозы, или, еще лучше, использовать встроенное машинное обучение (ML) для немедленного обнаружения и предотвращения новых угроз. Такой подход означает, что у вас есть согласованные меры защиты и политики безопасности во всех местах для ваших пользователей и ресурсов. Таким образом, у вас одинаковый уровень предотвращения угроз, независимо от того, работают ли ваши сотрудники из дома, в корпоративном офисе или в кафе. Кроме того, это обеспечивает безопасный доступ к данным из центра обработки данных, из удаленного филиала или из службы SaaS.

Это одна сторона истории. Другой, более значительный, заключается в том, что предотвращение угроз выходит за рамки обычной IPS и включает проверку всего трафика угроз, независимо от порта, протокола или шифрования. Затем он автоматически блокирует известные уязвимости, вредоносные программы,

эксплойты, шпионское ПО, а также управление и контроль (C2). Современное предотвращение угроз также все чаще использует встроенные методы машинного обучения для обнаружения и предотвращения новых неизвестных угроз до того, как они могут нанести ущерб.

Служба предотвращения угроз должна быть разработана таким образом, чтобы автоматически останавливать использование уязвимостей с помощью возможностей IPS. Он должен предлагать встроенную защиту от вредоносных программ и блокировать исходящий трафик C2. Другие услуги могут быть объединены с возможностями IPS для дополнительной защиты на каждом этапе жизненного цикла атаки, в том числе от известных и неизвестных угроз.

Одним из таких сервисов является облачный сервис анализа угроз, такой как WildFire от Palo Alto Networks. Это высокотехнологичный механизм анализа и предотвращения скрытых эксплойтов нулевого дня и вредоносных программ. Другие услуги включают фильтрацию URL-адресов и безопасность DNS для предотвращения веб-угроз, включая вредоносный контент и фишинговые страницы.

*Защита от уязвимостей*

Теперь посмотрим на защиту от уязвимостей. Национальный институт стандартов и технологий (NIST) и Национальная база данных уязвимостей (NVD) сообщили в 2020 году, что было обнаружено более 170 тысяч новых уязвимостей. Это число увеличилось более чем в 15 раз по сравнению с 2016 годом. Ваша служба предотвращения угроз должна предоставлять метод для обнаружения и блокировки использования этих уязвимостей программного обеспечения, которые теперь легко могут быть использованы злоумышленниками с помощью стандартных инструментов.

Любое современное решение по предотвращению угроз должно включать комплексную защиту от уязвимостей (эксплойтов и вредоносных программ) и предотвращения C2, которые в сочетании с основными интегрированными решениями, такими как песочница, встроенная защита на основе машинного обучения, расширенная защита URL-адресов и безопасность DNS, будут разумно устранять угрозы на каждом этапе атаки.

*Почему важны все основные возможности предотвращения угроз?*

Защита от уязвимостей предотвращает попытки использования уязвимостей, методы уклонения, попытки обфускации и другие известные уязвимости программного обеспечения. Это также должно включать защиту от попыток перебора, таких как сканирование портов, переполнение буфера и фрагментация протокола. Защита от вирусов и шпионского ПО нацелена на определенные известные семейства вредоносных программ и должна иметь возможность идентифицировать варианты, а не только определенные вредоносные файлы, которые легко изменить, чтобы избежать сигнатур на основе хэшей.

Защита управления и контроля предотвращает использование активности C2 для эксфильтрации данных, доставки вторичных вредоносных программ или предоставления дополнительных инструкций для будущих этапов атаки. Здесь также требуются передовые методы на основе машинного обучения, чтобы не отставать от растущего числа мобильных злоумышленников.

В заключение, обсуждаемые здесь меры предотвращения угроз обеспечивают высокий уровень защиты от известных угроз. Однако также важно учитывать операционные накладные расходы на управление системой сетевой безопасности. Единая комплексная платформа для подключения и защиты всего обеспечивает постоянную защиту и удобство работы, где бы ни находились приложения и пользователи. Это в вашей сети, в облаке или на мобильном устройстве. В идеале вам нужно лучшее в своем классе преобразование сети, защищенное от самых изощренных злоумышленников». ***(Jesse Ralston. Stopping threats in today's threat landscape // BNP Media (https://www.securitymagazine.com/articles/95448-stopping-threats-in-todays-threat-landscape). 18.06.2021).***

***

**«McDonald's, крупнейшая сеть ресторанов быстрого питания в мире, обнаружила утечку данных после того, как хакеры взломали ее системы и украли информацию, принадлежащую клиентам и сотрудникам из США, Южной Кореи и Тайваня.**

Как мировой розничный торговец общепитом, McDonald's обслуживает почти сотни миллионов клиентов каждый день в более чем 39 000 точек в более чем 100 странах, включая примерно 14 000 ресторанов только в США.

*Информация о платеже клиентов не раскрыта*

Сегодня компания заявила, что злоумышленники взломали ее системы на нескольких рынках по всему миру, что было обнаружено в результате расследования, проведенного внешними консультантами по безопасности.

McDonald's также сообщил сотрудникам из США, что злоумышленники могут украсть только деловую контактную информацию, принадлежащую сотрудникам США, и франшизы, которые не были личными или конфиденциальными, как впервые сообщил WSJ.

Злоумышленники также украли личную информацию (включая имена, адреса электронной почты, номера телефонов и адреса) у клиентов в Южной Корее и Тайване.

Однако количество клиентских документов, раскрытых в ходе инцидента, было небольшим, и нарушение никоим образом не повлияло на платежную информацию клиентов.

«Хотя мы смогли быстро закрыть доступ после идентификации, наше расследование показало, что доступ к небольшому количеству файлов был осуществлен, некоторые из них содержали личные данные», – говорится в заявлении McDonald's для BleepingComputer.

«Согласно нашему расследованию, только Корея и Тайвань имели доступ к личным данным клиентов, и они будут предпринимать шаги для уведомления регулирующих органов и клиентов, перечисленных в этих файлах.

«В этих файлах не содержалось никакой информации о платеже клиентов. В ближайшие дни несколько дополнительных рынков предпримут шаги для исправления файлов, содержащих личные данные сотрудников».

Сеть быстрого питания в настоящее время уведомляет затронутых клиентов и соответствующие органы на всех затронутых рынках.

McDonald's понимает важность эффективных мер безопасности для защиты информации, поэтому мы вложили значительные средства в реализацию нескольких инструментов безопасности в рамках нашей комплексной защиты от кибербезопасности. Эти инструменты позволили нам быстро выявлять и сдерживать недавние несанкционированные действия в нашей сети. Было проведено тщательное расследование, и мы работали с опытными третьими сторонами, чтобы поддержать это расследование. – Макдоналдс

*Не первое родео*

Это не первый раз, когда McDonald's сталкивается с инцидентом, связанным с безопасностью, за последние годы.

В 2017 году компания была вынуждена исправить уязвимость межсайтового скриптинга (XSS), затронувшую ее официальный сайт и раскрывающую пароли клиентов в виде обычного текста.

Как выяснил обнаруживший эту ошибку исследователь безопасности Тайме Гоммерс, злоумышленники могли использовать уязвимость, создав вредоносную ссылку.

При нажатии на цель он извлекает и расшифровывает данные пароля из локального файла cookie и отправляет их злоумышленнику в открытом виде.

Извлечение паролей любого пользователя стало возможным, потому что McDonald's хранила информацию о паролях в файле cookie, защищенном с помощью одного ключа и вектора инициализации для всех пользователей.

В связанных новостях игровой гигант Electronic Arts (EA) также подтвердил в четверг, что злоумышленники взломали его сеть и украли «ограниченное количество кода и связанных инструментов». ***(Sergiu Gatlan. McDonald's discloses data breach after theft of customer, employee info // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/mcdonalds-discloses-data-breach-after-theft-of-customer-employee-info/). 11.06.2021).***

***

**«Команда исследователей Check Point Research, подразделения Check Point Software Technologies, поставщика решений в области кибербезопасности, представила отчет Global Threat Index о самых активных угрозах в мае 2021 г.** CPR сообщает, что Trickbot, который впервые вошел в топ-лист в апреле 2019 г., теперь занял первое место, а Dridex (который был одной из самых популярных вредоносных программ в последние месяцы на фоне глобального всплеска программ-вымогателей), вышел из рейтинга. В России первое место занимает банковский троян Qbot – Trickbot сейчас на втором месте.

Пока не известно, почему Dridex не вошел в топ, но недавно были новости, что хакерская группировка Evil Corp (которая широко известна приверженностью Dridex), изменила свой подход к атакам, чтобы уклониться от преследования министерства финансов США.

Первое место в майском рейтинге занимает Trickbot — ботнет и банковский троян, который может красть финансовые и учетные данные, личную информацию. Он также способен распространять программы-вымогатели, например, Ryuk. Trickbot постоянно дополняется новыми возможностями, функциями и векторами

распространения. Это гибкое и настраиваемое вредоносное ПО, которое может распространяться в рамках многоцелевых кампаний. Trickbot стал особенно популярным после ликвидации ботнета Emotet в январе и попал в заголовки новостей на прошлой неделе, когда Министерство юстиции США предъявило обвинение гражданке Латвии за ее роль в создании и распространении Trickbot.

С начала 2021 г. команда CPR наблюдает значительный рост кибератак на предприятия. По сравнению с маем 2020 г. количество кибератак в Северной и Южной Америке увеличилось на 70%, в регионе EMEA — на 97%, а в Азиатско-Тихоокеанском регионе — ошеломляющее увеличение на 168% в годовом исчислении.

«Мы наблюдаем огромный рост числа кибератак, как в мире, так и в России. Это серьезная и очень тревожная тенденция, — сказал Василий Дягилев, глава представительства Check Point Software Technologies в России и СНГ. — Сейчас мы видим, что российские компании подвергаются серьезным атакам банковских троянов, например, таких как Trickbot и Qbot. Это одни из самых опасных угроз как в России, так и по всему миру. Они могут похищать платежные и учетные данные жертв, а также денежные средства с банковских счетов. Их атаки очень успешны, потому что они могут обходить механизмы защиты – например, двухфакторную аутентификацию. Часто для незаметной загрузки вредоносного ПО злоумышленники используют дропперы — программы, которые сами по себе не содержат вредоносный код и поэтому остаются незаметными для традиционных систем безопасности. Организации должны знать о рисках и заботиться о надежных решениях. Важно помнить, что лучше всего не обнаружить вовремя атаку, а предотвратить ее. При наличии правильных технологий большинство атак (и нулевого дня, и просто очень сложных) можно предотвратить, не нарушая бизнес-процессы».

Самое активное вредоносное ПО в мае 2021 в России: Qbot — банковский троян. Впервые появился в 2008 г., был предназначен для кражи банковских учетных данных и данных от нажатий клавиш у пользователей. Qbot часто распространяется через спам и использует несколько методов защиты от виртуальных машин и песочниц, чтобы затруднить анализ и уклониться от обнаружения. Затронул 21,5% организаций; Trickbot — один из доминирующих банковских троянов, который постоянно дополняется новыми возможностями, функциями и векторами распространения. Trickbot – гибкое и настраиваемое вредоносное ПО, которое может распространяться в рамках многоцелевых кампаний. Затронул 12% организаций; XMRig — программное обеспечение с открытым исходным кодом, впервые обнаруженное в мае 2017 г. Используется для майнинга криптовалюты Monero. Затронул 9% организаций.

Самое активное вредоносное ПО в мае 2021 в мире: в мае Trickbot стал самым популярным вредоносным ПО, атаковав 8% организаций по всему. За ним следуют XMRig и FormBook, затронувшие по 3% организаций каждый; Trickbot — один из доминирующих банковских троянов, который постоянно дополняется новыми возможностями, функциями и векторами распространения. Trickbot – гибкое и настраиваемое вредоносное ПО, которое может распространяться в рамках многоцелевых кампаний; XMRig — программное обеспечение с открытым

исходным кодом, впервые обнаруженное в мае 2017 г. Используется для майнинга криптовалюты Monero; FormBook — впервые обнаружен в 2016 г. Это инфостилер, предназначенный для ОС Windows. На подпольных хакерских форумах он позиционируется как MaaS из-за его развитых методов уклонения и относительно низкой цены. FormBook собирает учетные данные из различных веб-браузеров, делает снимки экрана, отслеживает и регистрирует на нажатие клавиш, а также может загружать и выполнять файлы в соответствии с приказами своего командного сервера.

Самые распространенные уязвимости в мае 2021 в мире: в этом месяце «Раскрытие информации в хранилище Git на веб-сервере» стала самой эксплуатируемой уязвимостью, затрагивающей 48% организаций во всем мире. На втором и третьем месте «Удаленное выполнение кода в заголовках HTTP (CVE-2020-13756)» и «Удаленное выполнение кода MVPower DVR» с охватом 47,5% и 46% соответственно.

Раскрытие информации в хранилище Git на веб-сервере — уязвимость в Git-репозитории, которая способствует непреднамеренному раскрытию информации учетной записи.

Удаленное выполнение кода в заголовках HTTP (CVE-2020-13756) — заголовки HTTP позволяют клиенту и серверу передавать дополнительную информацию с помощью HTTP-запроса. Злоумышленник может использовать уязвимый заголовок HTTP для запуска произвольного кода на устройстве жертвы.

Удаленное выполнение кода MVPower DVR — в устройствах MVPower DVR существует уязвимость удаленного выполнения кода. Злоумышленник может использовать ее для выполнения произвольного кода в уязвимом маршрутизаторе с помощью специально созданного запроса.

Самые активные мобильные угрозы в мае 2021: в этом месяце xHelper стал самым популярным вредоносным ПО для мобильных устройств. За ним следуют Triada и Hiddad.

xHelper — вредоносное приложение для Android, активно с марта 2019 г., используется для загрузки других вредоносных приложений и отображения рекламы. Приложение способно скрываться от пользовательских и мобильных антивирусных программ и переустанавливаться, если пользователь удаляет его.

Triada — модульный бэкдор для Android, предоставляющий права суперпользователя для загруженного вредоносного ПО.

Hiddad — модульный бэкдор для Android, который предоставляет права суперпользователя для загруженного вредоносного ПО, а также помогает внедрить его в системные процессы. Он может получить доступ к ключевым деталям безопасности, встроенным в ОС, что позволяет ему получать конфиденциальные данные пользователя.

Global Threat Impact Index и ThreatCloud Map разработаны ThreatCloud intelligence — совместной сетью по борьбе с киберпреступностью, которая предоставляет данные об угрозах и тенденциях атак из глобальной сети датчиков угроз. База данных ThreatCloud ежедневно проверяет более 3 млрд веб-сайтов, 600 млн файлов и выявляет более 250 млн вредоносных программ каждый день». ***(Дмитрий Степанов. Check Point Research назвала самое активное вредоносное***

***ПО мая 2021 года // CNews (https://safe.cnews.ru/news/line/2021-06-15_check_point_research_nazvala_samoe). 15.06.2021).***

***

**«В течение последней недели цифровые художники и создатели невзаимозаменяемых токенов (NFT) оказались в центре вредоносной кампании, в ходе которой злоумышленники пытаются похитить заработанные ими средства.**

Атаки начались на прошлой неделе и продолжались на выходных. О них стало известно после того, как пострадавшие художники начали активно сообщать в Twitter о том, что с их частных криптовалютных кошельков были похищены средства.

Судя по сообщениям, используя ряд подставных личностей, злоумышленники выдают себя за создателей NFT, предлагают бизнес-партнерство и обманом заставляют жертв загрузить на свои компьютеры и запустить вредоносный файл. Этот файл замаскирован под скринсейвер для Windows (.SCR).

Исследователь безопасности Барт Блейзер (Bart Blaze) изучил один из таких SCR-файлов и обнаружил, что он был сконфигурирован для временной установки на компьютерах жертв вредоносного ПО Redline. У вредоноса отсутствует механизм сохранения постоянства на системе, то есть, после перезагрузки компьютера он на нем не остается. Тем не менее, это не мешает Redline действовать молниеносно – вредонос способен собрать и похитить все пользовательские данные всего за несколько минут. В частности, он может похищать учетные данные для браузера и конфигурационные файлы криптовалютных кошельков, в том числе браузерные расширения.

В результате одной из таких атак злоумышленники похитили у жертвы 40 тыс. токенов AXS на сумму $176 тыс. Другие потеряли меньшие суммы, но ущерб, хоть и незначительный, все равно ущерб.

NFT – вид криптографических токенов, каждый экземпляр которых уникален (специфичен) и не может быть обменен или замещен другим аналогичным токеном, хотя обычно токены взаимозаменяемы по своей природе. NFT используются на нескольких платформах для подтверждения факта владения цифровыми активами и права их использования. Чаще всего речь идет о цифровых предметах, таких как экземпляры произведений компьютерного искусства, коллекционные цифровые предметы, online-игры». ***(Создатели NFT стали центром крупной фишинговой кампании // SecurityLab.ru (https://www.securitylab.ru/news/521338.php). 16.06.2021).***

***

**«Центр аналитики угроз Microsoft отслеживает новые действия злоумышленника NOBELIUM.** Наше расследование используемых методов и тактик продолжается, но мы видели спрей паролей и атаки методом перебора и хотим поделиться некоторыми подробностями, чтобы помочь нашим клиентам и сообществам защитить себя.

Эта недавняя деятельность была в основном неудачной, и большинство целей не были успешно скомпрометированы – на сегодняшний день нам известно о трех скомпрометированных объектах. Со всеми клиентами, которые были скомпрометированы или нацелены, связываются с помощью нашего процесса уведомления национального государства.

Этот вид деятельности не нов, и мы по-прежнему рекомендуем всем принимать меры безопасности, такие как включение многофакторной аутентификации для защиты своей среды от этой и подобных атак. Эта деятельность была нацелена на конкретных клиентов, в первую очередь ИТ-компании (57%), затем правительство (20%) и меньший процент для неправительственных организаций и аналитических центров, а также финансовых услуг. Деятельность была в основном сосредоточена на интересах США, около 45%, за которыми следовали 10% в Великобритании и меньшие числа из Германии и Канады. Всего было выбрано 36 стран.

В рамках нашего расследования этой продолжающейся деятельности мы также обнаружили вредоносное ПО для кражи информации на машине, принадлежащей одному из наших агентов поддержки клиентов, имеющей доступ к основной информации учетной записи для небольшого числа наших клиентов. В некоторых случаях субъект использовал эту информацию для запуска целенаправленных атак в рамках своей более широкой кампании. Мы быстро отреагировали, закрыли доступ и обезопасили устройство. Расследование продолжается, но мы можем подтвердить, что наши агенты поддержки настроены с минимальным набором разрешений, требуемых в рамках нашего подхода Zero Trust «наименее привилегированный доступ» к информации о клиентах. Мы уведомляем всех затронутых клиентов и поддерживаем их, чтобы их учетные записи оставались безопасными.

Это действие подчеркивает важность передовых мер безопасности, таких как архитектура с нулевым доверием и многофакторная аутентификация, и их важность для всех. Дополнительная информация о приоритетах передовой практики безопасности приведена ниже:

Управление доступом к удостоверениям

Нулевое доверие

Реализация моделей доступа с минимальными привилегиями». ***(New Nobelium activity // Microsoft Security Response Center (https://msrc-blog.microsoft.com/2021/06/25/new-nobelium-activity/). 25.06.2021).***

***

**«Киберпреступники все чаще используют виртуальные машины для взлома сетей с помощью программ-вымогателей.**

Используя виртуальные машины как часть процесса, злоумышленники могут выполнять свои действия с дополнительной тонкостью, поскольку запуск полезной нагрузки в виртуальной среде снижает шансы обнаружения активности – пока не станет слишком поздно и программа-вымогатель не зашифрует файлы на хост-машина.

В ходе недавнего расследования попытки атаки программ-вымогателей исследователи кибербезопасности Symantec обнаружили, что операции вымогателей использовали VirtualBox – легитимную форму программного обеспечения для виртуальных машин с открытым исходным кодом – для запуска экземпляров Windows 7 для помощи в установке программ-вымогателей.

«Мотивация, лежащая в основе этой тактики, – скрытность. Чтобы избежать подозрений или запуска антивирусного программного обеспечения, полезная нагрузка вымогателя будет «прятаться» внутри виртуальной машины при шифровании файлов на главном компьютере», – заявили в Symantec.

Несмотря на то, что виртуальная машина запускается отдельно от машины, на которой она размещена, она может иметь доступ к файлам и каталогам хост-машины через общие папки, которые киберпреступники могут использовать, чтобы позволить полезной нагрузке, размещенной на виртуальной машине, шифровать файлы на самом компьютере.

Хотя исследователи не смогли полностью идентифицировать программу-вымогатель, обнаруженную на виртуальной машине, сведения о том, как работала вредоносная программа, убедительно указывают на то, что это была Conti – печально известная форма вымогателя, используемая киберпреступниками в ряде громких кампаний., включая атаку программ-вымогателей на Службу здравоохранения Ирландии HSE.

Однако это была не единственная обнаруженная активность – исследователи обнаружили доказательства того, что злоумышленник пытался запустить программу-вымогатель Mount Locker на главном компьютере. Исследователи предполагают, что злоумышленник пытался запустить Conti через виртуальную машину, но, когда это не сработало, они переключились на использование Mount Locker.

Это не первый случай, когда банды вымогателей были замечены с использованием виртуальных машин для развертывания программ-вымогателей, но исследователи предупреждают, что это может значительно затруднить обнаружение атак.

«Группы часто подражают тактике других, если считают, что достигли успеха. Возможно, существует мнение, что некоторые решения безопасности не могут надежно и последовательно обнаруживать образец программы-вымогателя, выполняющийся изнутри виртуальной машины (ВМ)», – сказал Дик О'Брайен., руководитель группы Symantec Threat Hunter.

Хотя киберпреступники могут нацеливаться на устройства, на которых уже есть среды виртуальных машин, в этом случае создается впечатление, что они активно загружают инструменты, которые позволяют им работать. Одним из способов противодействия этому является мониторинг и контроль того, какое программное обеспечение установлено на машинах, поэтому потенциально вредоносные, но легитимные инструменты не могут быть загружены без разрешения.

«Используйте инструменты инвентаризации программного обеспечения и ограничения, которые позволяют им контролировать, какое лицензионное программное обеспечение может быть установлено. Кроме того, организации, уже

использующие программное обеспечение виртуальных машин, могут использовать корпоративные версии программного обеспечения, которые ограничивают создание новых неавторизованных виртуальных машин», – сказал О'Брайен». ***(Danny Palmer. Ransomware: Now gangs are using virtual machines to disguise their attacks // ZDNet (https://www.zdnet.com/article/ransomware-cyber-criminals-are-using-virtual-machines-to-hide-attacks-from-being-detected/). 24.06.2021).***

***

**«Zyxel, производитель корпоративных маршрутизаторов и VPN-устройств, выпустил предупреждение о том, что злоумышленники нацелены на его устройства и изменяют конфигурации для получения удаленного доступа к сети.**

В новой записке о поддержке компания сообщила, что «изощренный злоумышленник» нацелился на устройства безопасности Zyxel с удаленным управлением или включенным SSL VPN.

Атаки затрагивают организации, использующие Unified Security Gateway (USG), ZyWALL, объединенный межсетевой экран USG FLEX и VPN-шлюз, брандмауэры Advanced Threat Protection (ATP) и устройства серии VPN, на которых работает его прошивка ZLD.

«Злоумышленник пытается получить доступ к устройству через глобальную сеть; в случае успеха он обходит аутентификацию и устанавливает туннели SSL VPN с неизвестными учетными записями пользователей, такими как «zyxel_sllvpn», «zyxel_ts» или «zyxel_vpn_test», для управления конфигурацией устройства. Мы приняли меры сразу же после выявления инцидента», – отмечает Zyxel.

Похоже, это предполагает, что злоумышленники используют жестко заданные учетные записи для удаленного доступа к устройствам.

Ранее в этом году исследователи обнаружили в одном из бинарных файлов прошивки Zyxel жестко запрограммированную учетную запись администратора, из-за которой 100000 брандмауэров и VPN оказались открытыми для доступа в Интернет.

«Злоумышленник пытается получить доступ к устройству через глобальную сеть; в случае успеха он обходит аутентификацию и устанавливает туннели SSL VPN с неизвестными учетными записями пользователей, такими как «zyxel_sllvpn», «zyxel_ts» или «zyxel_vpn_test», для управления конфигурацией устройства. Мы приняли меры сразу же после выявления инцидента», – отмечает Zyxel.

Похоже, это предполагает, что злоумышленники используют жестко заданные учетные записи для удаленного доступа к устройствам.

Ранее в этом году исследователи обнаружили в одном из бинарных файлов прошивки Zyxel жестко запрограммированную учетную запись администратора, из-за которой 100000 брандмауэров и VPN оказались открытыми для доступа в Интернет.

Zyxel отмечает, что брандмауэры могут быть повреждены, если у пользователей возникают проблемы с доступом к VPN или с маршрутизацией, трафиком и входом в систему. Другие признаки включают неизвестные параметры конфигурации и проблемы с паролем.

Zyxel предупреждает администраторов об удалении всех неизвестных учетных записей администраторов и пользователей, созданных злоумышленниками. Он также советует им удалить неизвестные правила брандмауэра и политики маршрутизации.

Через Ars Technica клиент Zyxel разместил электронное письмо с раскрытием информации в Twitter.

«На основании проведенного до сих пор расследования мы считаем, что поддержание надлежащей политики безопасности для удаленного доступа в настоящее время является наиболее эффективным способом уменьшить поверхность атаки», – сказал Зиксель.

Рекомендуется отключить службы HTTP и HTTPS на стороне WAN. Тем, кому необходимо управлять устройствами со стороны WAN, рекомендуется ограничить доступ к надежному исходному интернет-адресу и включить фильтрацию GeoIP. Также подчеркивается, что администраторам необходимо изменить пароли и настроить двухфакторную аутентификацию.

Атаки на устройства Zyxel следует за серией аналогичных атак на ряд VPN-устройств, которые являются удобной точкой входа в корпоративную сеть для удаленных злоумышленников, чтобы получить постоянный доступ. В апреле Агентство по кибербезопасности и безопасности инфраструктуры США предупредило, что злоумышленники нацелены на уязвимости в VPN Pulse Secure Connect…». ***(Liam Tung. Sophisticated hackers are targeting these Zyxel firewalls and VPNs // ZDNet (https://www.zdnet.com/article/sophisticated-hackers-are-targeting-these-zyxel-firewalls-and-vpns/). 25.06.2021).***

***

**«Орган по надзору за окружающей средой Шотландии заявил, что для полного восстановления после кибератаки могут потребоваться годы.**

Агентство по охране окружающей среды Шотландии (Sepa) в канун Рождества похитило более 4000 цифровых файлов.

Генеральный директор Терри А'Хирн сообщил, что теперь он создает новую ИТ-систему с нуля.

Sepa заявила, что у нее есть системы резервного копирования, но пока не удалось восстановить все наборы экологических данных.

Он отклонил требование выкупа за атаку, которое требовала международная группа программ-вымогателей Conti. Затем украденные файлы были размещены в Интернете.

Государственный орган восстановил большинство своих ключевых услуг, таких как прогнозирование наводнений, но теперь строит новые ИТ-системы для их запуска.

Г-н А'Хирн сказал BBC Scotland: «Я думаю, что этот процесс займет год или два.

«В любом случае у нас были цели реформы, мы собирались постепенно строить новую ИТ-систему в течение пяти или шести лет.

«Это возможность, которую мы не хотели предоставлять со стороны преступников, но мы решили ускорить ее реализацию и построим ее через один или два года».

осила Sepa, есть ли у нее автономные резервные копии всех наборов данных, за которые она отвечает. Наблюдатель заявил, что вопрос будет решаться в соответствии с законами о свободе информации.

*Восстановление данных*

Ответ на этот запрос о свободе информации все еще не получен, но г-н А'Хирн сказал, что Sepa добилась значительных успехов в восстановлении своих наборов данных об окружающей среде из автономного хранилища.

Он сказал: «Как и у всех организаций, у нас было множество способов резервного копирования, мы восстановили подавляющее большинство наших наборов экологических данных – теперь мы снова работаем над ними в приоритетном порядке».

Часть затрат Sepa в размере 800 000 фунтов стерлингов на восстановление после кибератаки была связана с наймом специалистов по восстановлению данных.

Полиция Шотландии все еще расследует кибератаку и ранее указала на вероятную причастность к серьезной международной организованной преступности.

Джен Миллер Осборн из фирмы по кибербезопасности Palo Alto Networks сказала BBC Scotland, что группа Конти, заявившая об атаке, выделяется как «одна из самых жадных и агрессивных групп» в мире программ-вымогателей.

Она сказала, что Conti «агрессивно нацеливается на жертв и заранее исследует их» и ранее уже наносила удар по другим общественным организациям.

Она добавила: «Эта атака действительно показывает, что защитить себя от этих учетных записей становится все труднее.

«Как только они окажутся внутри, не займет много времени, прежде чем в ваших руках случится крупный инцидент». ***(Sepa cyber attack recovery could take years // BBC (https://www.bbc.com/news/uk-scotland-57578762). 24.06.2021).***

***

**«Все пять средних школ на острове Англси подверглись кибератаке.**

Совет сообщил, что нападение началось в среду.

Официальные лица заявили, что затронутые системы были отключены, чтобы «сдержать инцидент», но предупредили, что некоторые личные данные, в том числе электронные письма, могли быть скомпрометированы.

Исполнительный директор власти Аннвен Морган заявила, что в школах, скорее всего, будут проблемы.

Исгол Сыр Томас Джонс в Амлвче, Исгол Увхрадд в Бодедерне, Исгол Гифун Ллангефни, Исгол Дэвид Хьюз на мосту Менай и Исгол Увхрадд Каергиби в Холихеде – это школы, системы которых, как известно, были затронуты.

Г-жа Морган сказала: «Мы обнаружили кибератаку в среду и быстро приняли меры, чтобы привлечь группу специализированных консультантов по кибер-технологиям для расследования. Национальный центр кибербезопасности также будет оказывать нам поддержку в решении вопросов.

«Вероятно, в ближайшие недели в школах произойдут некоторые перебои, так как системы, возможно, потребуется восстановить, а другие останутся отключенными».

Она добавила: «Мы тесно сотрудничаем с другими партнерами, чтобы поддержать наши средние школы.

«Хотя в настоящее время мы не можем подтвердить факт утечки данных, Управление комиссара по информации также было проинформировано об этом инциденте». ***(Anglesey cyber-attack affects island's five secondaries // BBC (https://www.bbc.com/news/uk-wales-57603612). 25.06.2021).***

***

**«Геймеров обманывают, заставляя помогать хакерам разбогатеть, скачав игры со скрытыми вредоносными программами.**

Версии Grand Theft Auto V, NBA 2K19 и Pro Evolution Soccer 2018 бесплатно раздаются на форумах.

Но внутри кода этих игр спрятано вредоносное ПО для майнинга под названием Crackonosh, которое тайно генерирует цифровые деньги после загрузки игры.

По словам исследователей, преступники заработали на этой афере более 2 миллионов долларов (1,4 миллиона фунтов стерлингов).

Исследователи из Avast говорят, что «взломанные» игры быстро распространяют Crackonosh, и компания, занимающаяся разработкой программного обеспечения для кибербезопасности, теперь выявляет около 800 случаев на компьютерах каждый день.

Avast обнаруживает вредоносное ПО только на устройствах, на которых установлен его антивирус, поэтому реальное воздействие Crackonosh, вероятно, будет намного выше.

На данный момент вредоносное ПО было обнаружено более чем в десятке стран, в том числе:

Филиппины: 18 448 жертв

Бразилия: 16 584 жертвы

Индия: 13 779 жертв

Польша: 12727 жертв

США: 11 856 жертв

Великобритания: 8946 жертв

Когда Crackonosh установлен, он принимает меры для своей защиты, в том числе:

отключение обновлений Windows

удаление всего программного обеспечения безопасности

А программа майнинга криптовалюты, которую она затем запускает в фоновом режиме, без ведома владельца, может:

замедлить их компьютер

изнашивать компоненты из-за чрезмерного использования

увеличить счет жертвы за электроэнергию

«Crackonosh показывает, что попытки получить игры бесплатно могут дать вам то, чего вы не ожидали – вредоносное ПО», – сказал Кристофер Бадд из Avast.

«И мы видим, что это очень выгодно для авторов вредоносных программ».

По словам Avast, отслеживание цифровых кошельков хакеров показало, что мошенничество принесло более 2 миллионов долларов в криптовалюте Monero.

Компания полагает, что создателем вредоносного ПО может быть чех, отсюда и название Crackonosh, что в чешском фольклоре означает «горный дух».

В марте исследователи Cisco-Talos обнаружили вредоносное ПО внутри читерского ПО для нескольких игр.

А в начале этого месяца команда G Data Software обнаружила еще одну начинающую хакерскую кампанию, нацеленную на геймеров, использующих платформу Steam.

В своем последнем отчете о киберугрозах компания по кибербезопасности Akamai сообщает, что с 2019 года она обнаружила рост атак как на игровые бренды, так и на игроков, на 340%.

Многие из кибератак были связаны с кражей игровых аккаунтов из-за их ценных игровых предметов, которые затем продаются на хакерских форумах.

«Преступники все чаще атакуют геймеров», – сказал Стив Раган, исследователь безопасности Akamai.

«Геймеры известны тем, что тратят деньги на свое хобби, и они очень заинтересованы, что делает их постоянным источником добычи для криминальной экономики». ***(Joe Tidy. Crackonosh: How hackers are using gamers to become crypto-rich // BBC (https://www.bbc.com/news/technology-57601631). 25.06.2021).***

***

**«По словам исследователей Proofpoint, использование Cobalt Strike – законного, коммерчески доступного инструмента, используемого тестерами проникновения в сеть – киберпреступниками взлетело до небес.**

Исследователи зафиксировали рост числа реальных атак, в которых обнаружился Cobalt Strike, на 161 процент по сравнению с прошлым годом. Они стали свидетелями того, как этот инструмент использовался для нацеливания на десятки тысяч организаций, которыми владеет больше киберпреступников и операторов массового вредоносного ПО, чем участники продвинутых постоянных угроз (APT) или те операторы, которые предпочитают массовые вредоносные программы. Отчет опубликован во вторник.

Этот рост на 161 процент произошел в период с 2019 по 2020 год, но мошенники не утратили вкуса к Cobalt Strike в 2021 году: по словам исследователей, это все еще «массовая угроза».

Cobalt Strike отправляет маяки для обнаружения сетевых уязвимостей. При использовании по назначению имитирует атаку. Но злоумышленники выяснили, как использовать это против сетей для эксфильтрации данных, доставки вредоносных программ и создания поддельных профилей управления и контроля (C2), которые выглядят законными и не обнаруживаются.

Proofpoint – не единственная служба безопасности, которая заметила безудержный рост превращения Cobalt Strike в инструмент атаки: эволюция,

которая усилилась после того, как исходный код инструмента просочился из GitHub в ноябре 2020 года. Через два месяца после этой утечки, в январе 2021 года, Исследователи из Recorded Future зафиксировали всплеск использования взломанных или пробных версий Cobalt Strike, в основном известными APT-группами, включая APT41, Mustang Panda, Ocean Lotus и FIN7.

Исследователи Proofpoint обнаружили, что когда дело доходит до того, как злоумышленники пытаются скомпрометировать хосты, Cobalt Strike все чаще используется в качестве полезной нагрузки для начального доступа, а не в качестве инструмента второго этапа, который используется после того, как злоумышленники получили доступ. На самом деле, по их словам, «основная часть» кампаний Cobalt Strike в 2020 году была проведена преступниками.

Согласно отчету, при сопоставлении со структурой MITER Att & CK Proofpoint обнаружил, что Cobalt Strike появляется в цепочках атак во время начального доступа, выполнения и сохранения. «Основываясь на наших данных, Proofpoint с высокой степенью уверенности оценивает, что Cobalt Strike становится все более популярным среди злоумышленников в качестве полезной нагрузки для начального доступа, а не только как инструмент второго уровня, который злоумышленники используют после получения доступа, при этом преступники составляют большую часть приписываемых кампаний Cobalt Strike в 2020 году», – пишут исследователи.

*Роль Cobalt Strike в SolarWinds*

Cobalt Strike Beacon был одним из многих инструментов в обширном арсенале вредоносных программ, используемых в разрастающихся атаках цепочки поставок SolarWinds. В январе исследователи разоблачили часть связанного с SolarWinds вредоносного ПО, получившего название Raindrop, которое использовалось в целевых атаках после первоначального массового взлома Sunburst. Исследователи определили Raindrop – загрузчик бэкдора, который сбрасывает Cobalt Strike для выполнения бокового перемещения по сетям жертв – как один из инструментов, используемых для последующих атак.

Шпионская атака SolarWinds, которая затронула несколько правительственных агентств США, технологические компании, такие как Microsoft и FireEye, и многие другие, началась с отравленного обновления программного обеспечения, которое доставило бэкдор Sunburst примерно 18000 организациям весной 2020 года. злоумышленники (предположительно связанные с Россией) выбрали конкретные цели для дальнейшего проникновения, что они и сделали в течение нескольких месяцев. Компрометации были обнаружены в декабре 2020 года.

Правительство США считает атаки «вероятными» исходящими от Службы внешней разведки России: подразделения, в арсенале которого находится Cobalt Strike, «по крайней мере с 2018 года», согласно Proofpoint.

Этот инструмент существует уже почти десять лет и был выпущен в 2012 году как ответ на выявленные недостатки в популярной платформе тестирования на проникновение и взлома Metasploit. Как и Metasploit до этого, Cobalt Strike быстро подхватили и модифицировали злоумышленники: к 2016 году исследователи Proofpoint наблюдали, как Cobalt Strike используется в кибератаках.

Но исторически эти факторы угрозы представляли собой сложные APT-группы, такие как TA423 (также известные как Leviathan, APT40 или Gladolinium). Большинство кампаний Cobalt Strike, которые прошли в период с 2016 по 2018 год, были киберпреступными бандами или APT-группами, имеющими хорошие ресурсы. Но это соотношение резко упало в последующие годы, когда только 15 процентов кампаний Cobalt Strike приписывались известным злоумышленникам.

В Proofpoint говорится, что из приведенной ниже диаграммы видно, что количество угроз, содержащих Cobalt Strike, уменьшилось, но в годовом исчислении исследователи видели больше кампаний, связанных с Cobalt Strike в период с января по июнь 2021 года, чем с января по июнь 2020 года.

Как мошенники добиваются успеха в Cobalt Strike

Согласно отчету, киберпреступники могут забрать Cobalt Strike несколькими способами: они могут просто купить его на веб-сайте поставщика, что требует проверки. Согласно веб-сайту Cobalt Strike, новые лицензии Cobalt Strike стоят 3500 долларов за пользователя за годовую лицензию.

Кроме того, они могут купить версию в даркнете на хакерских форумах; или они могут получить взломанные незаконные версии программного обеспечения. В марте 2020 года злоумышленникам была предоставлена одна из таких взломанных версий Cobalt Strike 4.0. Годовая лицензия на взломанную версию, как сообщается, продавалась примерно за 45 000 долларов.

*Кобальтовый удар позволяет им жевать и трахаться*

Исследователи объяснили, что инструмент подходит для самых разных злоумышленников, поскольку он дешев и прост. По их словам, его можно быстро развернуть и ввести в действие, «независимо от уровня подготовки участников или доступа к человеческим или финансовым ресурсам».

Еще одно преимущество для преступников – то, что Cobalt Strike основан на сессиях. Другими словами, он позволяет вам войти, совершить грязные дела и выйти, не оставляя следов: «Если злоумышленники могут получить доступ к хосту и завершить операцию без необходимости постоянного сохранения, на нем не останется артефактов. хост после того, как он больше не работает в памяти», – описали исследователи. «По сути, они могут ударить и забыть».

Cobalt Strike также настраивается: это похоже на индивидуальный костюм мира вредоносных программ, позволяющий пользователям добавлять или удалять функции в соответствии с их целями или избегать обнаружения. APT29, например, «часто использует специальные загрузчики Cobalt Strike Beacon, чтобы слиться с легальным трафиком или избежать анализа», – пояснили исследователи.

Этот инструмент также отлично подходит для обфускации, поскольку и защитники, и злоумышленники используют один и тот же инструмент. «Если в организации есть красная команда, активно использующая это, возможно, вредоносный трафик может быть ошибочно принят за законный», – предположили исследователи.

Что касается простоты использования, это экономит время и усилия изощренных злоумышленников для создания собственного набора, исследователи продолжили: «Зачем тратить циклы разработки на что-то новое, если у вас уже есть отличный инструмент для работы?

*Фан-клуб Cobalt Strike*

В отчете приводится лишь небольшая выборка типов злоумышленников, отслеживаемых с помощью Cobalt Strike, в том числе:

TA800: крупная преступная группа, которую Proofpoint отслеживает с середины 2019 года, этот субъект пытается доставить и установить банковское вредоносное ПО или загрузчики вредоносных программ, такие как The Trick и BazaLoader.

TA547: Примерно с 2017 года эта группа также в первую очередь заинтересована в распространении банковских троянов, включая The Trick и ZLoader.

TA415: APT-актер, известный как Barium и APT41, который, как считается, связан с Китайской Народной Республикой. Proofpoint отслеживает, как этот субъект поставляет Cobalt Strike в качестве полезной нагрузки на первом этапе в середине 2020 года, а также участвует во многих других кампаниях, включая кампании против авиакомпаний в атаке на цепочку поставок с участием ИТ-провайдера SITA.

*Цепочка атак*

Кампании Cobalt Strike так же разнообразны, как и операторы, которые их запускают, используя различные приманки, типы угроз, дропперы, полезные нагрузки, пути атаки и варианты использования. Хотя использование этого инструмента в качестве начальной полезной нагрузки резко возросло, он также по-прежнему популярен как полезная нагрузка второго уровня. Исследователи Proofpoint писали, что он использовался вместе с вредоносными программами, такими как The Trick, BazaLoader, Ursnif, IcedID и многими другими популярными загрузчиками, когда первая вредоносная программа, которая пробирается через дверь, обычно загружается и выполняет Cobalt Strike.

Когда он доставляется напрямую, операторы используют такой же разнообразный набор методов, включая вооруженные документы Office, сжатые исполняемые файлы, PowerShell, динамический обмен данными (DDE), файлы HTA / HTML и системы распределения трафика.

После того, как он запущен и запущен и был установлен маяк для связи C2, злоумышленники попытались перечислить сетевые подключения и сбросить учетные данные Active Directory, пытаясь перейти в горизонтальном направлении к сетевому ресурсу, такому как контроллер домена, «позволяя развертывать программы-вымогатели для всех сетевых систем», – заявили исследователи.

Помимо сетевого обнаружения и сброса учетных данных, Cobalt Strike Beacon также может повышать привилегии, загружать и запускать дополнительные инструменты и внедрять эти функции в существующие запущенные хост-процессы, пытаясь избежать обнаружения.

*Ожидайте большего*

Данные Proofpoint показывают, что десятки тысяч организаций уже подверглись атаке Cobalt Strike, и, очевидно, нет ничего, что могло бы замедлить это растущее число в 2021 году.

*Это не вина Cobalt Strike*

В отчете также говорится, что в данных Proofpoint чаще встречаются и другие инструменты красной команды, в том числе Mythic, Meterpreter и Veil Framework.

Шеррод ДеГриппо, старший директор по исследованию и обнаружению угроз Proofpoint, сказал Threatpost, что такие инструменты безопасности, как эти и Cobalt Strike, не являются «злом по своей природе», но все же стоит изучить, «как незаконное использование фреймворков распространилось среди участников APT и как киберпреступники».

Она отметила, что использование общедоступных инструментов «согласуется с более широкой тенденцией, наблюдаемой Proofpoint: злоумышленники используют как можно больше законных инструментов, включая выполнение процессов Windows, таких как PowerShell и WMI [инструментарий управления Windows]; внедрение вредоносного кода в легитимные двоичные файлы; и частое использование допустимых сервисов, таких как Dropbox, Google Drive, SendGrid и Constant Contact, для размещения и распространения вредоносных программ.

«Это обсуждение, которое бушует в индустрии информационной безопасности в течение многих лет. «Агенты угроз во всем спектре криминального ПО и APT теперь полностью вооружены законными инструментами безопасности, и команды сражаются с наиболее подготовленными участниками угроз», – пояснила она.

«Наши данные показывают, что Cobalt Strike в настоящее время используется больше операторами киберпреступности и массового вредоносного ПО, чем злоумышленниками APT и шпионскими угрозами», – сказала она в заключение. «Это означает, что он стал широко распространенным в мире криминального ПО. Финансово мотивированные субъекты угрозы теперь вооружены так же, как те, которые финансируются и поддерживаются правительствами различных стран». ***(Lisa Vaas. Cobalt Strike Usage Explodes Among Cybercrooks // Threatpost (https://threatpost.com/cobalt-strike-cybercrooks/167368/). 29.06.2021).***

***

**«В год пандемии количество атак на игровую индустрию резко возросло: в 2020 году количество атак на веб-приложения увеличилось на 340 процентов.**

Согласно последнему отчету Akamai Technologies о состоянии Интернета и безопасности, Gaming in a Pandemic (PDF), трафик кибератак, нацеленный на индустрию видеоигр, взял верх в 2020 году, увеличившись с бешеной скоростью, опередившей все другие отрасли во время COVID-19. пандемия.

Игровая индустрия пострадала от более 240 миллионов атак на веб-приложения в 2020 году. Если быть точным, Akamai отследила 246 064 297 атак веб-приложений на игровую индустрию во всем мире, что составляет около 4 процентов из 6,3 миллиарда атак, отслеженных компанией за 2020 год., рост еще более резкий. С 2018 года Akamai стала свидетелем 415-процентного увеличения атак веб-приложений на игровую индустрию.

«Фактически, глобальное изменение атак на веб-приложения по сравнению с прошлым годом составило всего 2%, а это означает, что в 2020 году трафик атак в играх вырос больше, чем в любой другой отрасли», – говорится в отчете.

«Преступники безжалостны, и у нас есть данные, чтобы показать это», – цитируется в пресс-релизе Стив Раган, исследователь безопасности Akamai и автор отчета. «Мы наблюдаем удивительную настойчивость средств защиты индустрии видеоигр, которые проверяются ежедневно – а часто и ежечасно – преступниками, исследующими уязвимости, с помощью которых можно взломать серверы и раскрыть информацию. Мы также наблюдаем формирование множества групповых чатов в популярных социальных сетях, посвященных обмену методами и передовым опытом атак».

*Credential Stuffing также взорвался*

Но не только атаки на веб-приложения потрясли игровой мир. Атаки с заполнением учетных данных также увеличились на 224 процента по сравнению с 2019 годом. Как ни странно, количество атак с распределенным отказом в обслуживании (DDoS) снизилось почти на 20 процентов за тот же период.

Почему акцент делается на геймерах, на тех людях, которых в отчете Akamai называют «целенаправленной, очень заинтересованной и мотивированной демографией»? Очевидно, что геймеры – одна из любимых мишеней для «холодных и безжалостных» киберпреступников, как выразился Акамай.

Очевидно, что злоумышленники заинтересованы в злоупотреблениях в отношении игроков и игровой индустрии по разным причинам. Одним из наиболее заметных недавних инцидентов стало использование игровой платформы Steam для распространения вредоносного ПО. В прошлом месяце аналитики безопасности обнаружили вредоносное ПО, скрывающееся в метаданных файла изображения. Техника, называемая стеганографией, не нова, но ее использование на игровой платформе определенно ново.

Другая причина – деньги. В отчете упоминаются оценки аналитической компании Newzoo о том, что в 2021 году мировой игровой рынок достигнет 175 миллиардов долларов. Прогнозируется, что доходы от мобильных игр составят 52 процента от этой суммы, поскольку геймеры с готовностью обменивают реальные деньги на виртуальную валюту, которая будет использоваться в игре. такие предметы, как скины и индивидуальные улучшения персонажей.

Исследователи Akamai столкнулись с одной аферой, в которой преступники нацелились на компанию Codashop, один из крупнейших порталов пополнения баланса для геймеров, подделывая его сайт и используя его в качестве приманки для получения личной информации и учетных данных игроков.

Набор для фишинга Codashop собирал адреса электронной почты жертв, пароли, данные для входа в игру, имена пользователей в играх, данные геолокации, а также их уровень и уровень игрока, и все это для продажи на криминальных рынках.

*Мошенникам было так же скучно, как и всем остальным*

Что касается всплеска атак игровой индустрии в 2020 году, исследователи Akamai предположили, что вместо киберпреступников, мотивированных исключительно прибылью, в подполье, как и на земле, распространилась домашняя лихорадка эпохи пандемии.

По словам Алекса Бакштейна, архитектора отдела безопасности периферийных устройств в компании Imperva, занимающейся кибербезопасностью,

дело не всегда в деньгах. Скорее, эти атаки часто предназначены просто для того, чтобы подколоть геймеров. «В игровой сфере эти атаки редко мотивируются деньгами», – сказал он Threatpost в среду. «Чаще всего злоумышленники делают это, чтобы попасть под кожу других игроков или издателей, или, что еще хуже, просто для собственного развлечения, потому что они могут».

Это понятие совпадает с мыслями исследователей Akamai: они написали это, пытаясь выяснить «почему?» За этими свирепыми всплесками атак игровой индустрии мы не можем игнорировать тот факт, что 2020 год был «диким».

«Пока мы все были дома, приспосабливаясь к «новой норме», пытаясь сбалансировать работу, учебу и повседневную жизнь во время пандемии, многие люди обратились к играм как к выходу и средству личной связи», – говорит он. к отчету. «Преступники тоже сделали это. Не заблуждайтесь: хотя их намерения злы, они все же люди. Они разговаривали друг с другом, играли в игры, и в некоторых случаях эта социальная связь означала, что они в разной степени скоординировали свои усилия».

*Болтать о том, чтобы испортить всем игровое удовольствие*

Например, Akamai обнаружил групповые чаты о том, как преследовать игроков на популярной социальной платформе Discord – платформе, которая, несмотря на то, что она стоит, также популярна среди злоумышленников, которые используют ее для обхода безопасности, чтобы доставить кражи информации и - доступ к троянам (RAT) и другим вредоносным программам.

Исследователи Akamai обнаружили в групповых чатах Discord методы, инструменты и «лучшие практики» следующих основных векторов атак веб-приложений:

SQL-инъекция (SQLi)

Включение локального файла (LFI)

Межсайтовый скриптинг (XSS)

«Популярные обсуждения и учебные пособия были посвящены универсальным инструментам и использованию таких сервисов, как Shodan и Censys, для поиска баз данных, незащищенных активов и многого другого», – поясняется в отчете. «Ключом ко многим из этих обсуждений было использование известных инструментов и сервисов в качестве средства обфускации при поиске и сканировании».

*SQLi и LFI: лучшее оружие для автоматических атак*

В то время как количество атак на веб-приложения резко возросло, излюбленные векторы атак злоумышленников остались неизменными: Akamai обнаружил, что SQLi по-прежнему является вектором атаки номер один в игровой индустрии (59%), за ним следуют атаки LFI (24%).

Эти два основных вектора атаки в основном исходят от злоумышленников, которые автоматизировали свои усилия и ищут «оппортунистических ситуаций», – поясняется в отчете, – «когда новое приложение, API или функция учетной записи не были должным образом защищены и раскрыты.»

В отчете говорится, что основными целями для атак LFI и LFI являются мобильные и веб-игры, учитывая вероятное предположение злоумышленников, что

такие платформы – бездельник: они, вероятно, «не так надежно защищены, как их настольные и консольные аналоги». мышление идет.

Акамай сказал, что атаки LFI обычно пытаются раскрыть конфиденциальные детали в приложениях или службах, работающих на языках ASP, JSP или PHP. «Обычно атаки LFI приводят к раскрытию информации, такой как файлы конфигурации (которые могут использоваться для дальнейшего взлома сервера или учетных записей)», – отмечают исследователи. «В случае с игровой индустрией эти атаки могут раскрыть информацию об игроках или аккаунтах, которые могут быть использованы для обмана или эксплуатации».

Согласно отчету, когда атаки SQLi запускаются, в частности, в игровой индустрии, они могут привести к получению учетных данных для входа, личной информации или чего-либо еще, хранящегося в открытой базе данных. Затем злоумышленники продают эти учетные данные на торговых площадках Dark Web, где покупатели продолжают использовать их в атаках с заполнением учетных данных.

Атаки XSS и атаки с удаленным включением файлов (RFI) занимают третье место – 8% и 7% соответственно. «За последние три года это практически не изменилось», – говорится в отчете.

*За шипами атак стоят «придурки»*

Akamai изобразил несколько примечательных всплесков атак: 1 июня, а затем снова 11 июля 2020 года, когда Akamai зафиксировал 14,6 миллиона атак: число, которое превысило все количество атак в предыдущем месяце, всего за один день. Был еще один пик в сентябре, когда Akamai зафиксировал более 2 миллионов атак.

Как поясняется в отчете, компания не видела никакой «реальной, прямой связи с тем, что происходило в криминальном мире, и их внезапной взрывной концентрации на игровой индустрии».

Но ранее прошлым летом исследователи Akamai наблюдали, как на криминальных форумах распространяются несколько руководств. Эти руководства были посвящены автоматическим атакам SQLi и LFI, в том числе «придуркам», которые помогают злоумышленникам, не знакомым с этим типом атак, понять, что искать. Исследователи отметили, что «многие из этих руководств были пиратскими копиями установленных курсов обучения, таких как книги и курсы, предлагаемые SANS и Offensive Security, а также классы, преподаваемые в Udemy».

*Credential Stuffing*

Заполнение учетных данных составило около 6 процентов из 193 миллиардов атак, отслеженных Akamai во всем мире в прошлом году. Компания отследила 10 851 228 730 атак по подбору учетных данных в игровой индустрии: рост на 224% по сравнению с аналогичным периодом прошлого года. Эти атаки выросли на 24 процента за три года, с 2018 по 2020 год.

Компания Akamai связывает этот рост в некоторой степени с заметностью, которую она приобрела, поскольку за последний год добавила новых клиентов в свою глобальную сеть. Он обвиняет в атаках постоянных преступников, всплески которых произошли 11 апреля (76 миллионов), октябре (101 миллион) и декабре (157 миллионов).

«На втором месте после фишинга, заполнение учетных данных является наиболее распространенным типом атаки с захватом учетной записи, в основном из-за множества способов использования взломанной учетной записи злоумышленниками», – говорится в отчете. «Летом 2020 года массовые списки имен пользователей и паролей стоили всего 5 долларов за миллион записей».

В своем отчете об играх за 2020 год Akamai отметил, что преступники использовали время простоя во время карантина COVID-19, чтобы «переработать старые учетные списки и проверить их на соответствие новым целям», – пишут исследователи. Они начались в начале 2020 года и продолжались в течение всего года.

Заполнение учетных данных – «постоянная проблема», потому что у многих из нас такая вопиющая гигиена паролей, говорится в отчете. «Когда геймеры или общественность в целом повторно используют учетные данные на разных платформах и сервисах, успешная атака на одну из них напрямую приведет к успешной атаке на все другие места, где существует этот пароль», – говорится в сообщении.

По словам исследователей, это делает менеджеры паролей «необходимыми», учитывая, как они останавливают мошенников, пытаясь «переработать» пароли. «Если игровой пароль совпадает с паролем, используемым на веб-сайте банка, когда преступник взламывает одну учетную запись, он скомпрометирует их все, потому что этот повторно используемый пароль будет протестирован на нескольких платформах и службах», таких как учетные записи для потокового мультимедиа, они писали, что финансы и корпоративные активы.

*Нерфинг защиты*

Алекс Бакштейн из Imperva сообщил Threatpost, что наиболее часто используемым инструментом для защиты от ряда атак веб-приложений является межсетевой экран веб-приложений (WAF).

Когда дело доходит до XSS-атак, WAF «должен использовать фильтрацию на основе сигнатур для выявления и блокировки злонамеренных запросов», – отметил он.

Когда дело доходит до предотвращения атак SQLi, WAF полагается на большой и постоянно обновляемый список тщательно созданных сигнатур, которые позволяют ему «хирургическим путем отсеивать вредоносные SQL-запросы», – сказал он в электронном письме. Такой список обычно содержит сигнатуры для решения конкретных векторов атак и регулярно обновляется, чтобы ввести правила блокировки для вновь обнаруженных уязвимостей.

Он сказал, что когда дело доходит до RFI-атак, «дезинфекции ввода и надлежащих методов управления файлами почти никогда не бывает достаточно, даже если они эффективно минимизируют риск RFI». По его мнению, WAF, который отслеживает вводимые пользователем данные и отфильтровывает вредоносные запросы, используя комбинацию сигнатурных, поведенческих и репутационных эвристик безопасности, является «идеальным». «WAF развертывается как безопасный прокси-сервер и блокирует попытки RFI на границе сервера – до того, как они смогут взаимодействовать с вашим веб-приложением».

Бакштейн добавил, что современные WAF «должны быть интегрированы с другими решениями безопасности, такими как расширенная защита от ботов. От них WAF может получать дополнительную информацию, которая еще больше увеличивает его возможности безопасности. Например, брандмауэр веб-приложения, который обнаруживает подозрительный, но не явно злонамеренный ввод, может перепроверить его с данными IP, прежде чем принять решение о блокировке запроса. Он блокирует ввод, если сама IP имеет плохую репутацию». ***(Lisa Vaas. Pandemic-Bored Attackers Pummeled Gaming Industry // Threatpost (https://threatpost.com/attackers-gaming-industry/167183/). 23.06.2021).***

***

**«Microsoft в очередной раз успешно подверглась атаке с захватом зависимостей.**

Ранее, как впервые сообщил BleepingComputer, исследователь с этической точки зрения взломал более 35 крупных технологических компаний, включая Microsoft, используя уязвимость, называемую «путаница в зависимостях».

В этом месяце другой исследователь обнаружил внутреннюю зависимость npm, используемую проектом с открытым исходным кодом.

После публикации одноименной общедоступной зависимости он начал получать сообщения с серверов Microsoft.

*Взломана таинственная зависимость «быстрого поиска»*

На прошлой неделе исследователь Рикардо Ирамар душ Сантуш проводил аудит пакета SymphonyElectron с открытым исходным кодом на предмет ошибок, когда он обнаружил загадочную зависимость, используемую этим пакетом.

Эта зависимость называлась «быстрый поиск», но этого пакета не было в общедоступном реестре npmjs.com.

Осознав это, душ Сантуш зарегистрировал пакет с тем же именем в реестре npm, используя свой собственный код (показанный ниже в этой статье).

Предыдущие статьи BleepingComputer о путанице зависимостей объясняют, что этот термин представляет собой внутреннюю слабость различных менеджеров репозиториев с открытым исходным кодом, когда дело доходит до получения зависимостей, указанных для программного пакета.

Если проект использует частную, внутренне созданную зависимость, а зависимость с тем же именем существует и в общедоступном репозитории, это создаст «путаницу» для инструментов разработки в отношении того, какая зависимость упоминается.

Таким образом, общедоступная зависимость с тем же именем будет втягиваться в среду разработки вместо предполагаемой частной зависимости.

Таким образом, «путаница в зависимости» или атаки с перехватом позволяют злоумышленникам внедрить свой вредоносный код во внутреннее приложение в рамках автоматизированной атаки на цепочку поставок.

В марте этого года злоумышленники использовали эту технику для нацеливания на известные компании с помощью вредоносного кода, расширив сферу действия этой уязвимости за пределы мягкого исследования ошибок.

Поддельная версия пакета «swift-search», опубликованная dos Santos в рамках этого исследования, уже давно удалена из общедоступного реестра npm.

Однако, как исследователь безопасности Sonatype, я смог получить версию из автоматизированных систем обнаружения вредоносных программ Sonatype, где по состоянию на апрель 2021 года она была помечена как вредоносная…

Код, содержащийся в пакете душ Сантуш, получает доступ к чувствительным параметрам из системы, уязвимой для путаницы с зависимостями, и загружает их на PoC-сервер исследователя.

Эти поля и файлы включают:

Имя хоста системы и имя пользователя учетной записи

Переменные среды (env)

Название ОС и информация о версии

Общедоступный IP-адрес системы (IPv4 или IPv6)

/ etc / hosts файл

/ etc / passwd файл

/ etc / shadow файл

*Взломанный игровой сервер Microsoft Halo отвечает*

Через несколько часов после публикации пакета в реестре npm исследователь заметил, что серверы Microsoft получают ping-back.

«Запросы DNS поступали от 13.66.137.90, который является DNS-сервером Microsoft, а затем POST-запрос от 51.141.173.203, который также является IP-адресом от Microsoft (Великобритания)», – объясняет душ Сантуш в своем сообщении в блоге.

Исследователь утверждает, что доступ к https://51.141.173.203 предоставил ему сертификат SSL, в котором Microsoft была указана как организация, а в поле Common Name (CN) перечислено *.test.svc.halowaypoint.com.

Домен halowaypoint.com представляет серию видеоигр Halo, выпущенную Microsoft Xbox Game Studios.

Это еще раз подтвердило подозрения исследователя, что сервер Microsoft был успешно поражен его атакой с захватом зависимостей, и исследователь связался с Microsoft.

Некоторые данные, возвращаемые с сервера Microsoft, включали имя пользователя системы, пути к средам разработки приложений, различные идентификаторы и т. Д.

Хотя, как показано в приведенном выше коде, исследователь попытался также получить доступ к конфиденциальным системным файлам, включая / etc / passwd и / etc / shadow.

Как подтвердил BleepingComputer, сертификаты SSL, представленные на поддоменах halowaypoint.com, действительно указывают корпорацию Microsoft в качестве организации, стоящей за ними, а в записях WHOIS для 51.141.173.203 также указывается Microsoft в качестве ответственной организации…

Тем не менее, мы не смогли найти запись обратного просмотра, напрямую связывающую IP-адрес 51.141.173.203 с доменом Microsoft или SSL-сертификатом, что указывает на то, что IP-адрес мог быть отключен, согласно отчету исследователя.

BleepingComputer обратилась в Microsoft за комментариями, и нам сказали:

«Мы исследовали и определили, что основная проблема уже была решена до публикации отчета», – сказал BleepingComputer представитель Microsoft.

Кроме того, компания заявляет, что в этом отчете упоминается краткая проблема, вызванная сторонним изменением, и нет никаких указаний на какое-либо влияние на клиента.

За последний год количество атак на репозитории с открытым исходным кодом, включая npm, PyPI и RubyGems, неуклонно растет.

Теперь, когда в смесь добавлена путаница с зависимостями, и участники активно публикуют тысячи пакетов-подражателей в этих экосистемах, перед организациями и обслуживающими репозиториями возникла дополнительная проблема, связанная с пресечением злонамеренной активности». ***(Ax Sharma. Microsoft successfully hit by dependency hijacking again // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/microsoft-successfully-hit-by-dependency-hijacking-again/). 29.06.2021).***

***

**«McAfee, компания, занимающаяся кибербезопасностью от устройств к облаку, опубликовала отчет McAfee Threats Report: июнь 2021 года, в котором анализируется деятельность киберпреступников, связанных с вредоносным ПО и эволюция киберугроз в первом квартале 2021 года.**

Основные выводы:

• McAfee видит, что злоумышленники переходят от массовых кампаний к меньшему количеству более прибыльных целей;

• Количество вредоносных программ для майнинга криптовалюты выросло на 117% из-за роста 64-битных приложений CoinMiner;

• Новые варианты вредоносного ПО Mirai привели к росту угроз для Интернета вещей и Linux;

• Общее количество вновь обнаруженных вредоносных программ составляло в среднем 688 угроз в минуту.

В этом квартале киберпреступники перешли от низкодоходных массовых кампаний вымогателей к меньшему количеству настраиваемых кампаний вымогателей как услуги (RaaS), нацеленных на более крупные и прибыльные организации. Распространение 64-битных приложений CoinMiner привело к росту числа вредоносных программ для майнинга, генерирующих криптовалюту, на 117%. Кроме того, резкий рост числа новых вариантов вредоносного ПО на основе Mirai привел к увеличению числа вредоносных программ, нацеленных на системы Интернета вещей (55%) и Linux (38%).

«Преступники всегда будут совершенствовать свои методы, чтобы комбинировать любые инструменты, позволяющие им максимально увеличить денежную прибыль с минимальными сложностями и рисками», – сказал Радж Самани, научный сотрудник McAfee.

Каждый квартал McAfee оценивает состояние ландшафта киберугроз на основе углубленных исследований, следственного анализа и данных об угрозах,

собранных облаком McAfee Global Threat Intelligence с более чем миллиарда датчиков по множеству векторов угроз во всем мире.

*Программы-вымогатели*

В первом квартале количество программ-вымогателей сократилось на 50% отчасти из-за того, что злоумышленники перешли от широких кампаний, атакующих множество целей с использованием одних и тех же образцов, к кампаниям, атакующим меньшее количество крупных целей с использованием уникальных образцов. Кампании с использованием одного типа программ-вымогателей для заражения и вымогательства платежей от многих жертв, известны тем, что сотни тысяч систем со временем начинают распознавать и блокировать эти атаки. Позволяя злоумышленникам запускать уникальные атаки, партнерские сети RaaS дают возможность преступникам минимизировать риск обнаружения киберзащитой крупных организаций, а затем парализовать их и вымогать получение крупных платежей с использованием программ-вымогателей. Этот сдвиг отражается в сокращении числа известных типов семейств программ-вымогателей с 19 января 2021 года до 9 марта 2021 года.

Несмотря на громкие атаки со стороны группы DarkSide RaaS, выявленные во втором квартале 2021 года, в первом квартале чаще всего обнаруживался REvil, за ним следовали штаммы RansomeXX, Ryuk, NetWalker, Thanos, MountLocker, WastedLocker, Conti, Maze и Babuk.

*Вредоносное ПО для майнинга криптовалют*

В то время как известные атаки программ-вымогателей сосредоточили внимание на монетизации киберпреступлений с помощью платежей в криптовалюте, в первом квартале зафиксирован рост на 117% распространения вредоносных программ для майнинга, генерирующих криптовалюту, что можно объяснить резким скачком в 64-битных приложениях CoinMiner.

Вместо того, чтобы блокировать системы жертв и удерживать их в заложниках до тех пор, пока не будут произведены платежи в криптовалюте, вредоносное ПО Coin Miner заражает скомпрометированные системы и незаметно для владельца генерирует криптовалюту, используя вычислительные мощности этих систем. Преимущество для киберпреступников заключается в том, что ни от злоумышленника, ни от жертвы не требуется никакого взаимодействия. Хотя компьютеры жертвы могут работать медленнее, чем обычно, из-за загруженности программой-майнером, жертвы могут никогда не узнать, что их система создает денежную ценность для преступников.

*Угрозы и жертвы*

Общие угрозы вредоносного ПО:

В первом квартале 2021 года объем новых вредоносных угроз составил в среднем 688 угроз в минуту, что на 40 угроз в минуту больше, чем за четвертый квартал 2020 года.

*Устройства IoT и Linux*

Разнообразие новых вариантов вредоносного ПО Mirai привело к росту категорий вредоносных программ Интернета вещей (IoT) и Linux в первом квартале. Было замечено, что семейство Moobot (вариант Mirai) стало массовым и составляло несколько вариантов Mirai. Все эти варианты используют уязвимости в

устройствах Интернета вещей, таких как цифровые видеорегистраторы, веб-камеры и интернет-маршрутизаторы. После использования вредоносное ПО скрывается в системе, загружает более поздние его версии и подключается к командному серверу (C2). Когда скомпрометированные IoT-устройства подключены к их ботнетам, они могут быть привлечены к участию в DDoS-атаках.

*Отрасли промышленности*

McAfee зафиксировала 54%-ный рост публично сообщаемых киберинцидентов, нацеленных на технологический сектор в течение первого квартала 2021 года. За ними следуют секторы образования и финансового/страхового секторов с 46% и 41% соответственно, тогда как зарегистрированные инциденты в оптовом/розничном и государственном секторе снизились на 76% и 39% соответственно.

*Регионы*

Рост инцидентов зафиксирован по регионам: на 54% в Азии и на 43% в Европе, но количество киберугроз снизилось на 13% в Северной Америке. В то же время количество зарегистрированных инцидентов снизилось на 14% в Соединенных Штатах, а во Франции и Великобритании увеличилось на 84% и 19% соответственно». ***(Романов Роман. Отчёт: в 1-м квартале 2021 в Интернете вещей зафиксирован рост киберугроз от программ-вымогателей // Internetua (http://internetua.com/otcset-v-1-m-kvartale-2021-v-internete-vesxei-zafiksirovan-rost-kiberugroz-ot-programm-vymogatelei). 25.06.2021).***

***

## *Діяльність хакерів та хакерські угруповування*

---

**«Группа APT, которую мы называем BackdoorDiplomacy из-за основной вертикали ее жертв, нацелена на министерства иностранных дел и телекоммуникационные компании в Африке и на Ближнем Востоке по крайней мере с 2017 года. открытые устройства, такие как веб-серверы и интерфейсы управления сетевым оборудованием.** Попав в систему, ее операторы используют инструменты с открытым исходным кодом для сканирования окружающей среды и бокового движения. Интерактивный доступ достигается двумя способами: (1) через настраиваемый бэкдор, который мы называем Turian, который является производным от бэкдора Quarian; и (2) в меньшем количестве случаев, когда требуется более прямой и интерактивный доступ, развертываются определенные инструменты удаленного доступа с открытым исходным кодом. В некоторых случаях было замечено, что группа нацелена на съемные носители для сбора и утечки данных. Наконец, мишенью стали операционные системы Windows и Linux.

BackdoorDiplomacy имеет общие черты с несколькими другими азиатскими группами. Наиболее очевидной из них является связь между бэкдором турианцев и кварианцами. Конкретные наблюдения, касающиеся связи турианцев и кварианцев, записаны ниже в турианском разделе. Мы полагаем, что эта группа также связана с

группой, которую Касперский называет «CloudComputating», которая также была проанализирована Sophos.

Несколько жертв были скомпрометированы с помощью механизмов, которые очень похожи на кампании Rehashed Rat и MirageFox-APT15, задокументированные Fortinet в 2017 году и Intezer в 2018 году соответственно. Операторы BackdoorDiplomacy использовали свою особую форму перехвата порядка поиска DLL.

Наконец, метод сетевого шифрования, который использует BackdoorDiplomacy, очень похож на бэкдор, который Dr.Web вызывает Backdoor.Whitebird.1. Whitebird использовался для нацеливания на правительственные учреждения в Казахстане и Кыргызстане (оба являются соседями жертвы BackdoorDiplomacy в Узбекистане) в течение того же периода времени с 2017 года по настоящее время, в течение которого BackdoorDiplomacy была активна.

Quarian использовалась против сирийского министерства иностранных дел в 2012 году, а также против Государственного департамента США в 2013 году. Эта тенденция нацеливания на министерства иностранных дел продолжается и в Turian.

Жертвы были обнаружены в министерствах иностранных дел ряда африканских стран, а также в Европе, на Ближнем Востоке и в Азии. Дополнительные цели включают телекоммуникационные компании в Африке и по крайней мере одну ближневосточную благотворительную организацию. В каждом случае операторы использовали схожие тактики, приемы и процедуры (ДТС), но изменили используемые инструменты даже в пределах близких географических регионов, что, вероятно, затруднило отслеживание группы. На Рисунке 1 представлена карта жертв по странам и вертикали.

BackdoorDiplomacy нацелена на серверы с открытыми для доступа в Интернет портами, вероятно, используя незащищенные уязвимости или плохо обеспеченную безопасность загрузки файлов. В одном конкретном случае мы наблюдали, как операторы использовали уязвимость F5 BIP-IP (CVE-2020-5902), чтобы закрыть бэкдор Linux. В другом случае сервер Microsoft Exchange использовался через дроппер PowerShell, который установил China Chopper, хорошо известную веб-оболочку, используемую различными группами с 2013 года. В третьем мы наблюдали сервер Plesk с плохо настроенной защитой загрузки файлов. еще одна веб-оболочка, похожая на China Chopper. См. Рисунок 2 для обзора цепочки эксплойтов.

После первоначального компромисса во многих случаях группа BackdoorDiplomacy использовала разведку с открытым исходным кодом и инструменты красной группы для оценки среды на предмет дополнительных возможностей и бокового движения. Среди документированных инструментов:

EarthWorm, простой сетевой туннель с сервером SOCKS v5 и функциями передачи портов

Mimikatz и различные версии, включая SafetyKatz

Nbtscan, сканер NetBIOS из командной строки для Windows

NetCat, сетевая утилита, которая считывает и записывает данные через сетевые соединения.

PortQry, инструмент для отображения состояния портов TCP и UDP в удаленных системах

SMBTouch, используемый для определения уязвимости цели для EternalBlue.

Различные инструменты из дампа инструментов АНБ ShadowBrokers, включая, но не ограничиваясь:

ДаблПульсар

ВечныйСиний

EternalRocks

Вечный

Обычно используемые каталоги для размещения инструментов разведки и бокового перемещения включают:

C: \ Program Files \ Windows Mail \ en-US \

% LOCALAPPDATA% \ Microsoft \ InstallAgent \ Checkpoints \

C: \ ProgramData \ ESET \ ESET Security \ Logs \ eScan \

% USERPROFILE% \ ESET \ ESET Security \ Logs \ eScan \

C: \ Program Files \ hp \ hponcfg \

C: \ Program Files \ hp \ hpssa \

C: \ hp \ hpsmh \

C: \ ProgramData \ Mozilla \ updates \

Из перечисленных выше инструментов многие были обфусцированы с помощью VMProtect (v1.60-2.05), повторяющейся темы с инструментами BackdoorDiplomacy.

В некоторых случаях были замечены операторы, загружающие бэкдор-дропперы. Операторы различными способами пытались замаскировать свои бэкдор-дропперы и избежать обнаружения.

Соглашения об именах, предназначенные для использования в обычных операциях (например, amsc.exe, msvsvr.dll, alg.exe)

Размещение имплантатов в папках, названных для легального программного обеспечения (например, C: \ Program Files \ hp, C: \ ProgramData \ ESET, C: \ ProgramData \ Mozilla)

*Перехват порядка поиска DLL*

В одном из таких случаев операторы загрузили через веб-оболочку как ScnCfg.exe (SHA-1: 573C35AB1F243D6806DEDBDD7E3265BC5CBD5B9A), так и законный исполняемый файл McAfee, и vsodscpl.dll, вредоносную библиотеку DLL, названную в честь законной библиотеки DLL McAfee, вызываемой McAfee. exe. Развернутая версия vsodscpl.dll (SHA-1: FCD8129EA56C8C406D1461CE9DB3E02E616D2AA9) была вызвана ScnCfg.exe, после чего vsodscpl.dll извлек Turian, встроенный в свой код, записал его в память и выполнил.

В другой системе операторы сбросили на диск легитимную копию credwize.exe, мастера резервного копирования и восстановления учетных данных Microsoft, и использовали ее для выполнения вредоносной библиотеки New.dll, другого варианта Turian.

Около половины собранных нами образцов были обфусцированы с помощью VMProtect. Компиляция наблюдаемых команд оператора включена в раздел

Команды оператора. Уникальные схемы сетевого шифрования также отдельно обсуждаются ниже.

*Сходства с Quarian*

В первоначальном сообщении Касперского отмечается, что жертвы Quarian находились в сирийском Министерстве иностранных дел, аналогичной целевой группе Turian.

Во многих собранных нами образцах турианцев есть очевидное сходство с кварианскими. Оба используют мьютексы для проверки того, что работает только один экземпляр, хотя имена используемых мьютексов различаются. Мы наблюдали следующие мьютексы, используемые Турианом:

winsupdatetw

клиентыіх

клиент

updatethres

Прочие: динамически генерируются на основе имени хоста системы, ограничены восемью шестнадцатеричными символами, строчными буквами и начинаются с нуля в начале.

Домены и IP-адреса C&C серверов извлекаются с помощью аналогичных процедур XOR; где Quarian использует ключ дешифрования 0x44, Turian использует 0xA9.

И Turian, и Quarian читают первые четыре байта из файла cf в том же каталоге, что и исполняемый файл вредоносной программы, которые затем используются в качестве продолжительности сна в рамках процедуры передачи сигналов C&C.

Процесс подключения к сети Turian следует тому же шаблону, что и Quarian, пытаясь установить прямое подключение. Если это не удается из-за локального прокси с ответом 407 (требуется авторизация), оба пытаются использовать локально кэшированные учетные данные. Однако запрос, отправленный Turian на прокси, не содержит грамматических ошибок, отправленных Quarian...

Наконец, и Turian, и Quarian создают удаленную оболочку, копируя cmd.exe в alg.exe …

BackdoorDiplomacy – это группа, которая в первую очередь нацелена на дипломатические организации на Ближнем Востоке и в Африке и, реже, на телекоммуникационные компании. Их первоначальная методология атаки направлена на использование уязвимых приложений, доступных в Интернете, на веб-серверах с целью сброса и запуска веб-оболочки. После компрометации через веб-оболочку BackdoorDiplomacy развертывает программное обеспечение с открытым исходным кодом для разведки и сбора информации и поддерживает использование перехвата порядка поиска DLL для установки своего бэкдора Turian. Наконец, BackdoorDiplomacy использует отдельный исполняемый файл для обнаружения съемных носителей, вероятно, USB-флэш-накопителей, и копирования их содержимого в корзину основного диска.

BackdoorDiplomacy делится тактикой, приемами и процедурами с другими азиатскими группами. Turian, вероятно, представляет собой следующий этап эволюции Quarian, бэкдора, который последний раз использовался в 2013 году

против дипломатических целей в Сирии и США. Протокол сетевого шифрования Turian почти идентичен протоколу сетевого шифрования, используемому Whitebird, бэкдором, управляемым Calypso, другой азиатской группой. Whitebird был развернут в дипломатических организациях в Казахстане и Кыргызстане в то же время, что и BackdoorDiplomacy (2017-2020). Кроме того, BackdoorDiplomacy и APT15 используют одни и те же методы и тактики для установки своих бэкдоров в системы, а именно вышеупомянутый захват порядка поиска DLL.

BackdoorDiplomacy также является кроссплатформенной группой, ориентированной как на системы Windows, так и на Linux. Версия Turian для Linux имеет те же характеристики протокола сетевого шифрования и пытается вернуть оператору обратную оболочку TTY…» ***(Adam Burgher. BackdoorDiplomacy: Upgrading from Quarian to Turian // ESET (https://www.welivesecurity.com/2021/06/10/backdoordiplomacy-upgrading-quarian-turian/). 10.06.2021).***

***

**«Президент США Джо Байден допустив можливість покарання американських хакерів, які діють проти Росії…**

Американський лідер заявив після зустрічі лідерів G7 про необхідність притягати до відповідальності ті країни, які вкривають кіберзлочинців.

«США відкриті для пропозиції про притягнення до відповідальності своїх кіберзлочинців, що діють проти Росії», – повідомив Байден.

Він зазначив, що його надихнули коментарі російського президента Володимира Путіна про те, що Росія готова екстрадувати кіберпрестуників в США на взаємній основі, якщо Вашингтон зробить те ж саме.

«Ми домовилися спільно працювати над кіберзагрозами, такими як програми – вимагачі, і притягнути до відповідальності країни, які вкривають кіберзлочинців», – додав американський лідер…» ***(Американських хакерів, що діють проти Росії, можуть покарати // Слово і Діло (https://www.slovoidilo.ua/2021/06/13/novyna/svit/amerykanskyx-xakeriv-diyut-proty-rosiyi-mozhut-pokaraty). 13.06.2021).***

***

**«Корейский научно-исследовательский институт атомной энергии вчера сообщил, что их внутренние сети были взломаны в прошлом месяце северокорейскими злоумышленниками с использованием уязвимости VPN.**

Корейский научно-исследовательский институт атомной энергии, или KAERI, является спонсируемым правительством институтом по исследованию и применению ядерной энергии в Южной Корее.

О взломе впервые сообщили в начале этого месяца, когда южнокорейские СМИ Sisa Journal начали освещать нападение. В то время KAERI сначала подтвердил, а затем отрицал факт нападения.

В заявлении и на пресс-конференции, проведенных вчера KAERI, институт официально подтвердил факт нападения и извинился за попытку скрыть инцидент.

*Приписывается северокорейским террористам*

KAERI заявляет, что атака произошла 14 июня после того, как северокорейские злоумышленники взломали их внутреннюю сеть, используя уязвимость VPN.

KAERI заявляет, что они обновили скрытое устройство VPN, чтобы исправить уязвимость. Однако журналы доступа показывают, что тринадцать различных неавторизованных IP-адресов получили доступ к внутренней сети через VPN.

Один из этих IP-адресов связан с спонсируемой государством Северной Кореей хакерской группой, известной как «Кимсуки», которая, как полагают, работает в разведывательном агентстве Северокорейского разведывательного управления.

В октябре 2020 года CISA опубликовала предупреждение о группе APT Kimsuky и заявила, что им «вероятно, поручают северокорейский режим глобальную миссию по сбору разведданных».

Совсем недавно Malwarebytes опубликовал отчет о том, как Kimsuky (также известная как Thallium, Black Banshee и Velvet Chollima) активно атакует правительство Южной Кореи, используя бэкдор AppleSeed в фишинговых атаках.

«Одна из использованных Kimsuky приманок под названием «на корейском языке переводится как «Министерство иностранных дел, издание 2021-05-07», что указывает на то, что она была разработана для Министерства иностранных дел Южной Кореи», – поясняет отчет Malwarebytes о недавних действиях злоумышленника.

«Согласно собранным нами данным, мы определили, что это одна из организаций, представляющих большой интерес для Кимсуки».

Malwarebytes заявляет, что Kimsuky в ходе недавних фишинговых атак нацелился на другие южнокорейские правительственные учреждения, в том числе:

Министерство иностранных дел Республики Корея 1-й секретарь

Министерство иностранных дел Республики Корея 2-й секретарь

Министр торговли

Заместитель генерального консула в Генеральном консульстве Кореи в Гонконге

Сотрудник по ядерной безопасности Международного агентства по атомной энергии (МАГАТЭ)

Посол Посольства Шри-Ланки в государстве

Советник Министерства иностранных дел и торговли

KAERI заявляет, что они все еще расследуют атаку, чтобы подтвердить, к какой информации был получен доступ». ***(Lawrence Abrams. South Korea's Nuclear Research agency hacked using VPN flaw // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/south-koreas-nuclear-research-agency-hacked-using-vpn-flaw/). 19.06.2021).***

***

**«Ко взлому компьютерных систем норвежского правительства в 2018 году может быть причастна хакерская группировка APT31, спонсируемая Китаем, об этом заявила глава отдела контрразведки Службы безопасности**

**норвежской полиции (PST) Ханне Бломберг (Hanne Blomberg) в интервью телеканалу NRK.**

«В данном случае у нас есть информация, четко указывающая на причастность группы APT31 к операции против правительственной администрации», – отметила Бломберг.

На минувшей неделе PST опубликовала новые подробности о взломе IT-систем Стортинга (норвежский парламент). Согласно пресс-релизу ведомства, злоумышленникам удалось получить права администратора для доступа к централизованным компьютерным системам, используемым всеми правительственными органами в стране и похитить некоторые данные. Предполагается, что в руки хакеров попали в том числе логины и пароли сотрудников правительства.

Расследование не выявило признаков хищения секретной информации или персональных данных граждан Норвегии, сообщила PST. Хотя в пресс-релизе ведомство не уточнило, кто именно стоит за взломом Стортинга, отмечается, что атака может быть делом рук группировки, взломавшей компьютерную сеть норвежского облачного провайдера Visma AS летом 2018 года». ***(Полиция Норвегии заявила о причастности китайских хакеров ко взлому правительства в 2018 году // SecurityLab.ru (https://www.securitylab.ru/news/521495.php). 20.06.2021).***

***

## *Вірусне та інше шкідливе програмне забезпечення*

---

**«В мае 2021 года Национальный координационный центр по компьютерным инцидентам (НКЦКИ) ФСБ России совместно с Ростелеком объявили, что несколько российских государственных структур стали жертвами APT-кампании.** Хотя российское правительство и раньше делало подобное заявление, оно впервые сопровождает его умеренно подробным техническим анализом. Несколько исследователей, в том числе и я, ухватились за возможность написать наши правила YARA и надеются увидеть виновника.

Твиттер-вселенная InfoSec не нуждалась в таких артефактах, поскольку слепые спекуляции немедленно указывали на западное правительство, Five Eyes или Соединенные Штаты как фактических виновников. Я думаю, мы с облегчением узнаем, что это, скорее всего, не так – хотя бы потому, что мы привыкли ожидать более высоких стандартов для разработки западных вредоносных программ.

Первоначальные попытки найти образцы оказались безрезультатными, но в минувшие выходные ситуация изменилась, когда какая-то добрая душа (или, что более вероятно, автоответчик) загрузила копию вредоносного ПО Mail-O на VirusTotal. Мы отслеживаем эту активность под названием «ThunderCats».

В соответствии с выводами отчета НКЦКИ-Ростелеком, вредоносная программа Mail-O действует как загрузчик с тонкой внешностью, похожей на легитимную программу Mail.ru Disk-O. Маскировка состоит из номера версии («19.05.0045»), взятого из легитимного исполняемого файла Disk-O, и

использования реального Mail.ru для публикации сведений о жертве и размещения полезной нагрузки следующего этапа.

Размер исполняемого файла увеличен до 2,8 МБ за счет статического связывания libcurl 7.64.1 и OpenSSL. Сосредоточение становится важным, чтобы не попасть в бессмысленную кроличью нору, обращая вспять несвязанный открытый исходный код. По этой причине мы должны сосредоточиться в первую очередь на экспортируемых функциях…

ServiceMainпринимает имя службы в качестве аргумента и пытается зарегистрировать обработчик управления службой с определенной HandlerProcфункцией, предназначенной для проверки и установки статуса этой службы. Имея действительный дескриптор состояния службы, Mail-O отключает вызывающий процесс от своей консоли, изменяет значения состояния службы, чтобы отразить его текущее состояние выполнения, и вызывает Enteryфункцию. Обратите внимание на ServiceMainфункцию со строкой отладки «ServiceMain Load» – шаблон, который используется при поиске соединений с другими вредоносными программами.

*Mail-O: Entery*

EnteryФункция вызывается в конце ServiceMain, но он также может быть независимо друг от друга вызывается. Он проверяет наличие ‘%AllUsersProfile%\PSEXESVC.EXE’и запускает его как процесс. Эта функция зарегистрирована как фильтр исключений верхнего уровня.

Основная Enteryлогика организована в следующей функции. Сначала Mail-O проверяет реестр на наличие установленной легитимной программы Mail.Ru Disk-O. Он расшифровывает строки конфигурации и контакты https://dispatcher.cloud.mail.ru/.

Mail-O использует SystemTime для POST зашифрованного имени хоста жертвы (или, в случае его отсутствия, строки «[none]») и получения полезной нагрузки. Перед запуском полезная нагрузка записывается во временный путь. Затем Mail-O переходит в режим ожидания до определенного времени.

Нам еще предстоит увидеть Webdav-O, другой вредоносный компонент, описанный в отчете Ростелеком-Solar. Однако это не должно помешать нам последовать интересному примеру.

*Связь с Entery*

Mail-O экспортирует функцию с именем Entery, предположительно с ошибкой «Entry». Орфографические ошибки – настоящий подарок для исследователей вредоносных программ. Как оказалось, это не первый случай, когда в недавно развернутом вредоносном ПО отмечается орфографическая ошибка.

В декабре 2020 года Игнасио Санмиллан и Матье Фау опубликовали отличный отчет об атаке на систему поставок во Вьетнаме, в которой использовалось вредоносное ПО PhantomNet (также известное как SManager). Исследователи отметили, что устойчивость вредоносного ПО была установлена с помощью запланированной задачи, которая называла экспорт вредоносной библиотеки DLL «Entery». Исследователи отмечают, что на этот же экспорт указала NTT Security в своем анализе вредоносного ПО TManger, которое они, в свою очередь, коррелируют с злоумышленником Proofpoint TA428. Это невзрачное имя

злоумышленника было принято Dr.Web в сообщениях о недавних атаках на дополнительные российские цели, включая исследовательские институты.

Хотя все это может показаться немного запутанным, я репетирую логические связи, чтобы проиллюстрировать два момента:

Существует устоявшаяся история того, что этот весьма незападный «субъект угрозы» нацелился на азиатские и российские цели.

Эти предположительно китайские группы деятельности сбивают с толку, и их трудно распутать. Инструментальные средства, вероятно, совместно используются несколькими участниками угроз (вероятно, включая PhantomNet / SManager), и то, что называется «TA428», вероятно, является объединением нескольких групп угроз.

Для скептиков ниже мы предоставили правило YARA для Enteryперекрытия, которое влечет за собой не только имя функции экспорта, но также общий макет функции и некоторые общие строки. Обратите внимание, что макет, вероятно, был разработан итеративно на основе шаблона с открытым исходным кодом.

Наконец, хотя я быстро осуждаю качество вредоносного ПО, считая его не соответствующим высоким западным стандартам, важно отметить, что ThunderCats (и более крупный зонтик TA428) успешно проводят атаки на цепочки поставок, ориентированные на конкретные регионы. они намного превосходят их вес в своих усилиях по сбору разведданных, и их не следует недооценивать как противника». ***(JUAN ANDRÉS GUERRERO-SAADE. ThunderCats Hack the FSB | Your Taxes Didn't Pay For This Op // SentinelOne (https://labs.sentinelone.com/thundercats-hack-the-fsb-your-taxes-didnt-pay-for-this-op/). 08.06.2021).***

***

**«Check Point Research (CPR) сообщила о бэкдоре, который совершенствовался на протяжении последних трёх лет и был внедрён в целях шпионажа в Windows-компьютеры Министерства иностранных дел одного из правительств Юго-Восточной Азии**

Атака начиналась с сообщений целевого фишинга, приходящих якобы от адресатов из госаппарата. При попытке жертвы открыть имеющие официальный вид документы, скачивались шаблоны.RTF, инфицированные при помощи инструментария Royal Road. Популярный у китайских киберпреступных группировок, Royal Road эксплуатирует уязвимости CVE-2017-11882, CVE-2018-0798 и CVE-2018-0802 редактора уравнений Microsoft Word.

Внедрённый в RTF-файл скрипт вместе с зашифрованной вредоносной нагрузкой создаёт отложенное задание Windows Update и выполняет другие маневры противодействия «песочнице». Кроме того он отсылает предварительную информацию о жертве на командный сервер (C2). Если её сочтут интересной, начинается второй этап атаки, на котором собственно загружается бэкдор оригинальной разработки под внутренним именем VictoryDll_x86.dll.

Это ПО способно выполнять множество функций, ориентированных на шпионаж, в том числе чтение/запись/удаление файлов, запуск команд через cmd.exe, захват экрана, создание/завершение процессов, получение имён окон верхнего уровня, ключей реестра, содержимого таблиц UDP/TCP, детальной

информации о пользователе и компьютере, а также отключение ПК. Добытые сведения переправляются на командный сервер американского провайдера, начальные же этапы кибератаки координируют серверы, находящиеся в Гонконге и в Малайзии.

«Злоумышленников интересуют не только холодные данные, но и то, что происходит на персональном компьютере цели в любой момент, – комментирует глава службы аналитики угроз в CPR, Лотем Финкельстин (Lotem Finkelsteen). – Хотя мы смогли заблокировать описываемую тут операцию слежения за властями страны в Юго-Восточной Азии, вполне возможно, что преступная группа использует свое новое оружие кибершпионажа против других целей по всему миру». ***(Новое китайское киберорружие опробовано на правительстве соседней страны // Компьютерное Обозрение (https://ko.com.ua/novoe_kitajskoe_kiberoruzhie_oprobovano_na_pravitelstve_sosednej_strany_137613). 07.06.2021).***

***

**«Компания Eset обнаружила новую версию сложного вредоносного ПО Gelsevirine, которое принадлежит группе киберпреступников Gelsemium. Среди целей этой угрозы – государственные учреждения, религиозные организации, производители электроники и университеты Восточной Азии и Ближнего Востока.**

До последнего времени Gelsemium в основном удавалось избегать обнаружения. Специалисты Eset начали отслеживать деятельность группы с середины 2020 г., хотя судя по всему она активна еще с 2014 г.

Деятельность группы является целенаправленной из-за небольшого количества жертв, а возможности вредоносного ПО указывают на то, что злоумышленники занимаются кибершпионажем. В частности, группа Gelsemium имеет много адаптированных компонентов.

Киберпреступники используют три компонента и систему плагинов, в частности загрузчики Gelsemine и Gelsenicine, а также основной плагин Gelsevirine, которые предоставляют широкие возможности для сбора информации.

Исследователи Eset считают, что Gelsemium причастна к атаке на компанию BigNox, которая известна как операция NightScout. Эта атака на цепь поставки была направлена на компрометацию механизма обновления NoxPlayer, эмулятора Android для компьютеров Windows и Mac, который является частью продуктовой линейки BigNox с более чем 150 млн. пользователей во всем мире.

В ходе исследования было выявлены некоторые сходства между этой атакой и активностью группы Gelsemium. В частности, жертвы атаки на цепь поставки впоследствии были скомпрометированы Gelsemium. Кроме этого, зафиксировано сходство определенных версий вредоносных программ, которые применялись в обеих атаках». ***(Хакеры группы Gelsemium атакуют госучреждения, производителей электроники и университеты // Компьютерное Обозрение(https://ko.com.ua/hakery_gruppy_gelsemium_atakuyut_gosuchrezhdeniya_proizvoditelej_jelektroniki_i_universitety_137654). 10.06.2021).***

***

**«Эксперты кибербезопасности сообщили о Siloscape, первом известном вредоносном ПО, которое заражает кластеры Kubernetes в облачных средах, атакуя контейнеры Windows Server.**

Даниэль Призман (Daniel Prizmant) из Unit 42, отмечает: «Siloscape – это сильно запутанная вредоносная программа, нацеленная на кластеры Kubernetes через контейнеры Windows. Её основная цель – открыть бэкдор в плохо сконфигурированные кластеры Kubernetes для запуска вредоносных контейнеров».

Впервые обнаруженное в марте 2021 года ПО Siloscape использует множество методов, включая атаку на распространенные облачные приложения, такие как веб-серверы. Проникая через известные уязвимости оно, затем, использует техники выхода из контейнера Windows и получает возможность удалённого выполнения кода на базовом узле.

После этого вредоносная программа пытается распространиться по кластеру, пользуясь учётными данными узла, и создаёт через Tor-прокси анонимное соединение со своим командным и управляющим (C2) сервером. Последний выдаёт дальнейшие инструкции, такие как кража криптовалюты или конфиденциальных данных из приложений Kubernetes.

В отличие от прочих контейнерных угроз, Siloscape само по себе не вредит работе кластера, а, наоборот, старается чтобы создание «чёрного хода» осталось никем не замеченным.

Unit 42 утверждает, что обнаружила 23 активных жертвы после того, как ей удалось получить доступ к C2-серверу Siloscape, который имел 313 пользователей. Судя по дате запуска этого сервера, кампания Siloscape стартовала 12 января 2020 года.

Для защиты от этой угрозы администраторам следует проверить настройки безопасности: в правильно защищённом кластере Kubernetes разрешений узлов недостаточно для создания нового развёртывания. В этом случае Siloscape останавливается». ***(Обнаружен первый бэкдор для контейнеров Windows // Компьютерное Обозрение (https://ko.com.ua/obnaruzhen_pervyj_bjekdor_dlya_kontejnerov_windows_137668). 10.06.2021).***

***

**«…В четверг исследователи Sophos заявили, что они обнаружили кампанию вредоносных программ, которая не следует типичным поведенческим моделям: проникновение в систему, кража информации, банковское мошенничество и т.д. – вместо этого вредоносное ПО «блокирует возможность зараженных пользователей посетите большое количество веб-сайтов, посвященных пиратскому программному обеспечению».**

Способы распространения варьируются: некоторые образцы были похоронены в архивах, замаскированных под программные пакеты, продвигаемые через чат-сервис Discord, тогда как другие распространяются напрямую через торрент.

По словам главного исследователя Эндрю Брандта, создатель использовал названия многочисленных брендов программного обеспечения, игр, инструментов повышения производительности и решений для кибербезопасности, чтобы скрыть вредоносное ПО, и поэтому, похоже, нацелен на всех, от геймеров до профессионалов, которые могут не захотеть покупать программное обеспечение. лицензия.

Вредоносные пакеты имеют имена в общепринятых форматах, используемых при распространении пиратского программного обеспечения, например «Minecraft 1.5.2 Cracked [Полная установка] [Онлайн] [Список серверов]». Файлы помечаются как загруженные из The Pirate Bay.

«Файлы, которые кажутся размещенными в системе обмена файлами Discord, как правило, представляют собой отдельные исполняемые файлы», – говорит Брандт. «Те, которые распространяются через Bittorrent, были упакованы способом, который более похож на то, как пиратское программное обеспечение обычно распространяется с использованием этого протокола: добавлено в сжатый файл, который также содержит текстовый файл и другие вспомогательные файлы, а также старомодный Интернет-ярлык. файл."

Если дважды щелкнуть исполняемый файл вредоносной программы, появится всплывающее сообщение, в котором говорится, что в системе жертвы отсутствует важный файл.DLL. В фоновом режиме вредоносная программа получает дополнительную полезную нагрузку, получившую название ProcessHacker, с внешнего веб-сайта. Эта полезная нагрузка отвечает за изменение файла HOSTS на целевой машине.

Процесс блокировки пиратских веб-сайтов вредоносным ПО является элементарным, поскольку он просто добавляет список от нескольких сотен до более чем 1000 веб-доменов и указывает им на адрес локального хоста. Как ни странно, некоторые веб-сайты, внесенные в черный список, не имеют никакого отношения к пиратству.

Однако на современных машинах могут потребоваться привилегии для изменения файла HOSTS, и не каждый образец запускает системы Windows для повышения привилегий вредоносного ПО. Когда эта эскалация не произошла, модификация файла HOSTS завершилась неудачно.

«Изменение файла HOSTS – грубый, но эффективный метод предотвращения доступа компьютера к веб-адресу», – говорит Sophos. «Это грубо, потому что, хотя вредоносная программа работает, у нее нет механизма сохранения. Любой может удалить записи после того, как они были добавлены в файл HOSTS».

В некоторые пакеты вредоносного ПО оператор добавил файлы, входящие в комплект установщика, что, вероятно, улучшит его легитимность как пиратский программный пакет. Большинство этих файлов представляют собой нежелательный код и изображения мусора, хотя обычный файл.nfo содержит расистские оскорбления.

«На первый взгляд, цели и инструменты противника предполагают, что это могла быть какая-то грубо скомпилированная операция линчевателей по борьбе с пиратством», – прокомментировал Брандт. "Однако обширная потенциальная целевая аудитория злоумышленника – от геймеров до профессионалов бизнеса – в

сочетании с любопытным сочетанием устаревших и новых инструментов, TTP и причудливым списком веб-сайтов, заблокированных вредоносным ПО, – все это составляет конечную цель этой операции. немного мутно».

Хотя вредоносная программа является примитивной и не оказывает серьезного воздействия на пользователей – если они не поклонники взломанного программного обеспечения или пиратского контента – если файл HOSTS был изменен, Sophos утверждает, что его можно очистить, запустив Блокнот от имени администратора, открыв c: \ Windows \ System32 \ Drivers \ etc \ hosts и удалив ссылки». ***(Charlie Osborne. This strange malware stops you from visiting pirate websites // ZDNet (https://www.zdnet.com/article/this-strange-malware-stops-you-from-visiting-pirate-websites/). 17.06.2021).***

***

**«Злоумышленники, стоящие за вредоносным ПО, известным как SolarMarker, используют PDF-документы, заполненные ключевыми словами для поисковой оптимизации (SEO), чтобы повысить их видимость в поисковых системах, чтобы привести потенциальных жертв к вредоносному ПО на вредоносном сайте, который выдает себя за Google Диск.**

По заявлению Microsoft, SolarMarker – это вредоносная программа-бэкдор, которая крадет данные и учетные данные из браузеров.

SEO-отравление – это метод старой школы, который использует поисковые системы для распространения вредоносного ПО. В этом случае злоумышленники используют тысячи PDF-файлов, заполненных ключевыми словами и ссылками, которые перенаправляют неосторожных пользователей с нескольких сайтов на тот, который устанавливает вредоносное ПО.

«Атака работает с использованием PDF-документов, предназначенных для ранжирования в результатах поиска. Для этого злоумышленники дополнили эти документы более чем 10 страницами ключевых слов по широкому кругу тем, от «страховая форма» и «принятие контракта» до «как чтобы присоединиться к SQL» и «математическим ответам», – говорится в твите Microsoft Security Intelligence.

Crowdstrike забил тревогу по поводу SolarMarker в феврале за то, что он использовал ту же тактику отравления SEO. Вредоносная программа в основном нацелена на пользователей в Северной Америке.

Злоумышленники размещали страницы на сайтах Google в качестве приманки для вредоносных загрузок. Сайты продвигали загрузку документов и часто занимали высокие позиции в результатах поиска, опять же для повышения рейтинга поиска.

Исследователи Microsoft обнаружили, что злоумышленники начали использовать Amazon Web Services (AWS) и сервис Strikingly, а также сайты Google.

«При открытии PDF-файлы предлагают пользователям загрузить файл.doc или версию.pdf желаемой информации. Пользователи, которые переходят по ссылкам, перенаправляются через 5–7 сайтов с такими TLD, как.site,.tk и.ga». Сказал Microsoft.

«После нескольких перенаправлений пользователи попадают на контролируемый злоумышленником сайт, имитирующий Google Диск, и их просят загрузить файл».

Обычно это приводит к вредоносному ПО SolarMarker / Jupyter, но Microsoft также видела, что случайные файлы загружаются как часть очевидного метода уклонения от обнаружения, добавил он.

Он передает украденные данные на командный сервер и продолжает работать, создавая ярлыки в папке «Автозагрузка», а также изменяя ярлыки на рабочем столе.

«Данные Microsoft 365 Defender показывают, что метод отравления SEO эффективен, учитывая, что антивирус Microsoft Defender обнаружил и заблокировал тысячи этих PDF-документов во многих средах», – заявили в Microsoft». ***(Liam Tung. This data and password-stealing malware is spreading in an unusual way // ZDNet (https://www.zdnet.com/article/this-data-and-password-stealing-malware-is-spreading-in-an-unusual-way/). 14.06.2021).***

***

**«Исследователи обнаружили новый бренд вредоносного ПО, предназначенное для взлома контейнеров Windows с целью достижения кластеров Kubernetes.**

Вредоносная программа, получившая название Siloscape, считается необычной, поскольку вредоносная программа, обычно предназначенная для нацеливания на контейнеры, ориентирована на Linux как на популярную операционную систему для управления облачными приложениями и средами.

Согласно подразделению 42 Palo Alto Networks, Siloscape, впервые обнаруженный в марте этого года, был назван так потому, что его общая цель – выйти из контейнеров Windows через изолированное хранилище серверов.

В понедельник в блоге исследователи кибербезопасности заявили, что Siloscape использует прокси-сервер Tor и домен.onion для подключения к своему командному серверу (C2), который злоумышленники используют для управления вредоносным ПО, кражи данных и отправки команды.

Вредоносная программа, обозначенная как CloudMalware.exe, нацелена на контейнеры Windows – используя сервер, а не изоляцию Hyper-V – и будет запускать атаки с использованием известных уязвимостей, которые не были исправлены для первоначального доступа к серверам, веб-страницам или базам данных.

Затем Siloscape попытается добиться удаленного выполнения кода (RCE) на базовом узле контейнера, используя различные методы выхода из контейнера Windows, такие как олицетворение CExecSvc.exe, службы образов контейнера, для получения привилегий SeTcbPrivilege.

«Siloscape имитирует привилегии CExecSvc.exe, олицетворяя свой основной поток, а затем вызывает NtSetInformationSymbolicLink для вновь созданной символической ссылки, чтобы выйти из контейнера», – сообщает Unit 42. «Более конкретно, он связывает свой локальный контейнерный диск X с диском C хоста».

Если вредоносному ПО удастся сбежать, оно затем попытается создать вредоносные контейнеры, украсть данные из приложений, работающих в скомпрометированных кластерах, или загрузит майнеры криптовалюты, чтобы использовать ресурсы системы для тайного майнинга криптовалюты и получения прибыли операторами до тех пор. поскольку деятельность остается незамеченной.

Разработчики вредоносной программы позаботились о том, чтобы существовала серьезная обфускация – до такой степени, что функции и имена модулей деобфускируются только во время выполнения – для того, чтобы скрыть себя и усложнить обратное проектирование. Кроме того, вредоносная программа использует пару ключей для расшифровки пароля сервера C2 – ключи, которые предположительно генерируются для каждой уникальной атаки.

«Жестко запрограммированный ключ делает каждый двоичный файл немного отличным от остальных, поэтому я нигде не смог найти его хэш», – говорится в исследовании. «Это также делает невозможным обнаружение Siloscape только по хешу».

Блоку 42 удалось получить доступ к C2 и идентифицировать в общей сложности 23 активных жертвы, а также в общей сложности 313 жертв, вероятно, обеспеченных в ходе кампаний за последний год. Однако прошло всего несколько минут, прежде чем присутствие исследователей было замечено, их выгнали с сервера, а сервис стал неактивным – по крайней мере, на этом адресе.onion.

Microsoft рекомендует развертывать контейнеры Hyper-V, если контейнеризация используется как форма границы безопасности, а не полагаться на стандартные контейнеры Windows. Модуль 42 добавил, что кластеры Kubernetes должны быть правильно настроены и не должны допускать, чтобы одних привилегий узлов было достаточно для создания новых развертываний». ***(Charlie Osborne. Siloscape: this new malware targets Windows containers to access Kubernetes clusters // ZDNet (https://www.zdnet.com/article/siloscape-this-new-malware-targets-windows-containers-to-access-kubernetes-clusters/). 07.06.2021).***

***

**«Разработчик-линчеватель меняет положение с пиратами программного обеспечения, распространяя вредоносное ПО, которое не позволяет им получить доступ к сайтам с пиратским программным обеспечением в будущем.**

Злоумышленники обычно используют пиратское программное обеспечение и поддельные сайты взлома для распространения вредоносного ПО среди ничего не подозревающих пользователей, которые думают, что скачивают последнюю игру или фильм.

Вредоносные программы распространяются через эти методы, как правило, информацию о краже трояны, вымогатели или cryptominers, которые могут быть использованы для генерации значения для угрозы актера.

*Вредоносное ПО блокирует доступ к The Pirate Bay*

В новом отчете SophosLabs рассказывает о распространении вредоносного ПО, которое не позволяет пиратам получить доступ к самому популярному торрент-сайту с защищенным авторским правом контенту – The Pirate Bay.

«В одном из самых странных случаев, которые я видел за последнее время, один из моих коллег по лаборатории недавно рассказал мне о кампании вредоносных программ, основная цель которой, похоже, отклоняется от наиболее распространенных мотивов вредоносных программ». объясняет в новом отчете главный исследователь SophosLabs Эндрю Брандт.

«Вместо того, чтобы пытаться украсть пароли или вымогать у владельца компьютера выкуп, это вредоносное ПО блокирует доступ компьютеров зараженных пользователей к большому количеству веб-сайтов, посвященных пиратскому программному обеспечению, путем изменения файла HOSTS в зараженной системе».

По словам Брандта, новое вредоносное ПО распространяется через Discord или торрент-сайты пиратского ПО. В Discord вредоносное ПО распространяется как отдельные исполняемые файлы, которые притворяются пиратским ПО…

На таких сайтах, как The Pirate Bay, вредоносное ПО распространяется аналогично другим торрент-файлам в том смысле, что они содержат файлы readme, файлы NFO и файлы ярлыков обратно на thepiratebay.org.

Однако многие файлы, содержащиеся в этих торрент-архивах, не служат никакой цели и добавляются только в качестве наполнителя для имитации типичного торрент-файла с пиратским программным обеспечением или фильмами.

«При более внимательном рассмотрении этих файлов, связанных с установщиком, становится ясно, что они не имеют никакой практической пользы, кроме как придать архиву вид файлов, которые обычно используются через Bittorrent, и изменить значения хэшей с добавлением случайных данных», – говорит Брандт. в своем отчете.

Когда пользователь запускает исполняемый файл вредоносной программы, он изменяет файл Windows HOSTS, добавляя многочисленные записи, указывающие на 127.0.0.1 для сайтов, связанных с The Pirate Bay.

После добавления этих записей HOSTS, когда пользователь пытается получить доступ к одному из перечисленных сайтов, они вместо этого будут перенаправлены на свой локальный хост и не смогут подключиться к фактическому IP-адресу сайта. Это эффективно блокирует доступ к перечисленным сайтам, которые распространяют торренты для контента, защищенного авторским правом.

Что еще хуже, при запуске вредоносного ПО Vigilante оно подключается к удаленному узлу, находящемуся под контролем злоумышленника, и отправляет имя поддельного пиратского программного обеспечения, которое заразило пользователя.

Поскольку веб-серверы обычно регистрируют IP-адрес посетителя, злоумышленник теперь имеет как IP-адрес пирата, так и название программного обеспечения или фильма, которые они пытались использовать.

Хотя неизвестно, для чего эта информация используется, злоумышленники могут поделиться ею с интернет-провайдерами, агентствами по авторскому праву или даже правоохранительными органами.

Злоумышленники также могут использовать эту информацию в дальнейших атаках, таких как кампании по вымогательству по электронной почте, когда

злоумышленник угрожает раскрыть незаконную деятельность пользователя, если они не заплатят небольшое требование о вымогательстве.

Брандт сообщил BleepingComputer, что эта вредоносная кампания велась с октября 2020 года по январь 2021 года, когда сайт злоумышленника отключился.

По словам Брандта, вредоносные торренты также перестали распространяться, вероятно, после того, как пользователи перестали их рассылать, узнав, что файлы являются вредоносными или поддельными.

В прошлом, хоть и редко, но бдители брали правосудие в свои руки, взламывая Netgear для удаления вредоносных программ, распространяя вредоносные программы для защиты IoT-устройств, выпуская вооруженные версии». ***(Lawrence Abrams. Vigilante malware blocks victims from downloading pirated software // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/vigilante-malware-blocks-victims-from-downloading-pirated-software/). 17.06.2021).***

***

**«Microsoft подтвердила подписание вредоносного драйвера, распространяемого в игровых средах.**

Этот драйвер, названный «Netfilter», на самом деле является руткитом, который, как было замечено, обменивался данными с китайскими IP-адресами управления и контроля (C2).

Аналитик вредоносного ПО G Data Карстен Хан впервые обратил внимание на это событие на прошлой неделе, и к нему присоединилась более широкая информационная служба. Сообщество по отслеживанию и анализу вредоносных драйверов с печатью Microsoft.

Этот инцидент в очередной раз выявил угрозы безопасности цепочки поставок программного обеспечения, но на этот раз он возник из-за слабости процесса подписи кода Microsoft.

Драйвер Netfilter – руткит, подписанный Microsoft.

На прошлой неделе системы оповещения о кибербезопасности G Data отметили ложное срабатывание, но это не так – подписанный Microsoft драйвер под названием «Netfilter».

Рассматриваемый драйвер был замечен в обмене данными с базирующимися в Китае IP-адресами C&C, не обеспечивающими законной функциональности, и поэтому вызвал подозрения.

Именно тогда Карстен Хан, аналитик вредоносных программ G Data, поделился этим публично и одновременно связался с Microsoft…

«Начиная с Windows Vista, любой код, работающий в режиме ядра, необходимо тестировать и подписывать перед общедоступным выпуском, чтобы обеспечить стабильность операционной системы».

«Драйверы без сертификата Microsoft не могут быть установлены по умолчанию», – заявляет Хан.

В то время BleepingComputer начал наблюдать за поведением URL-адресов C2, а также обратился в Microsoft за заявлением.

Первый URL-адрес C2 возвращает набор дополнительных маршрутов (URL-адресов), разделенных вертикальной чертой ("|")…

По словам Хана, каждое из них служит определенной цели:

URL-адрес, заканчивающийся на "/ p", связан с настройками прокси-сервера,

"/ s" предоставляет закодированные IP-адреса перенаправления,

"/час?" для получения CPU-ID,

"/ c" предоставил корневой сертификат, и

"/ v?" связано с функцией самообновления вредоносного ПО.

Например, BleepingComputer видит "/ v?" path предоставил URL-адрес самого вредоносного драйвера Netfilter, о котором идет речь (находится в "/ d3")…

Исследователь G Data потратил некоторое время на тщательный анализ драйвера и пришел к выводу, что он является вредоносным.

Исследователь проанализировал драйвер, его функции самообновления и индикаторы взлома (IOC) в подробном сообщении в блоге.

«В образце есть процедура самообновления, которая отправляет свой собственный хэш MD5 на сервер через hxxp: //110.42.4.180: 2081 / v? V = 6 & m =», – говорит Хан…

«Затем сервер отвечает URL-адресом последнего образца, например, hxxp: //110.42.4.180: 2081 / d6, или« OK », если образец актуален. Вредоносная программа заменяет свой собственный файл соответствующим образом», далее объяснил исследователь.

В ходе анализа к Хану присоединились другие исследователи вредоносных программ, в том числе Иоганн Айдинбас, Такахиро Харуяма и Флориан Рот.

Рот смог собрать список образцов в электронную таблицу и предоставил правила YARA для их обнаружения в ваших сетевых средах.

Примечательно, что IP-адрес C2 110.42.4.180, к которому подключается вредоносный драйвер Netfilter, принадлежал Ningbo Zhuo Zhi Innovation Network Technology Co., Ltd, согласно записям WHOIS…

Microsoft признала, что подписала вредоносный драйвер

Microsoft активно расследует этот инцидент, хотя пока нет доказательств того, что использовались украденные сертификаты для подписи кода.

Несчастный случай, похоже, возник в результате того, что злоумышленник следил за процессом Microsoft по отправке вредоносных драйверов Netfilter и сумел законным образом получить подписанный Microsoft двоичный файл: «Microsoft расследует злоумышленника, распространяющего вредоносные драйверы в игровых средах».

«Актер представил драйверы для сертификации через программу совместимости оборудования Windows. Драйверы были созданы третьей стороной».

«Мы приостановили действие учетной записи и проверили отправленные ими сообщения на предмет наличия дополнительных признаков вредоносного ПО», – заявила вчера Microsoft.

По данным Microsoft, злоумышленник в основном нацелился на игровой сектор, особенно в Китае, с помощью этих вредоносных драйверов, и пока нет никаких признаков того, что корпоративные среды были затронуты.

Microsoft пока воздерживается от приписывания этого инцидента субъектам национального государства.

Изощренные злоумышленники могут злоупотреблять ложно подписанными двоичными файлами для облегчения крупномасштабных атак на цепочку поставок программного обеспечения.

Многогранная атака Stuxnet, направленная на ядерную программу Ирана, знаменует собой хорошо известный инцидент, в ходе которого сертификаты подписи кода были украдены у Realtek и JMicron для облегчения атаки.

Однако этот конкретный инцидент выявил слабые места в законном процессе подписания кода, которые злоумышленники использовали для получения кода, подписанного Microsoft, без нарушения каких-либо сертификатов». ***(Ax Sharma. Microsoft admits to signing rootkit malware in supply-chain fiasco // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/microsoft-admits-to-signing-rootkit-malware-in-supply-chain-fiasco/). 26.06.2021).***

***

***Програми-вимагачі***

---

**«Positive Technologies проанализировала актуальные киберугрозы I квартала 2021 г. и зафиксировала рост числа атак с помощью программ-вымогателей, появление множества новых шифровальщиков.**

Отмечается, что разработчики вредоносного ПО все чаще стали адаптировать его под атаки на средства виртуализации.

По данным анализа, количество атак увеличилось на 17% в сравнении с I кварталом 2020 г., а относительно IV квартала 2020 г. прирост составил 1,2%. При этом 77% атак были целенаправленными, а инциденты с частными лицами составили 12% от числа всех инцидентов. Чаще всего злоумышленники атаковали госучреждения, промышленность и организации в сфере науки и образования.

В исследовании говорится, что программы-вымогатели остаются самым распространенным вредоносным ПО. Их доля среди прочего ВПО, применяемого в атаках на организации, увеличилась на семь процентных пунктов в сравнении с IV кварталом 2020 г. и составляет 63%. Эксперты компании также отметили появление новых шифровальщиков, например, Cring, Humble и Vovalex. При этом сообщается об активности шифровальщика WannaCry, громко заявившего о себе в 2017 г.

Разработчики вредоносного ПО продолжают искать новые способы обхода средств защиты. Сообщается, что для этого они используют редкие языки программирования. Как, например, в случае с создателями ВПО для удаленного управления BazarBackdoor, которые переписали его, используя язык Nim, или операторами программ-вымогателей Vovalex и RobbinHood, которые изначально выбрали редкие языки D и Golang.

По данным исследования, суммы выкупа, требуемые операторами программ-вымогателей продолжают расти, а из-за того, что некоторые компании отказываются от уплаты выкупа, злоумышленники изобретают новые тактики

вымогательства: например, если компания не собирается платить, преступники угрожают сообщить о факте атаки и об украденных данных ее клиентам: по замыслу преступников, клиенты смогут повлиять на компанию и заставить ее заплатить — чтобы не допустить разглашения своих данных.

Все больше злоумышленников разрабатывают свое ВПО для проведения атак на среды виртуализации, а некоторые пытаются активно эксплуатировать уже найденные уязвимости в ПО для развертывания виртуальной инфраструктуры. Прежде всего, эксперты связывают это с глобальным процессом переноса ИТ-инфраструктуры компаний в виртуальную среду». ***(Злоумышленники ориентируют вредоносы под атаки на виртуальную инфраструктуру // Компьютерное Обозрение (https://ko.com.ua/zloumyshlenniki_orientiruyut_vredonosy_pod_ataki_na_virtualnuyu_infrastrukturu_137693). 14.06.2021).***

***

**«Бразильская компания JBS USA Holdings Inc. выплатила выкуп в размере 11 миллионов долларов киберпреступникам, которые на прошлой неделе временно вывели из строя предприятия, на которых перерабатывается примерно одна пятая часть поставок мяса в стране, сказал исполнительный директор компании.**

Выплата выкупа в биткойнах была произведена для защиты мясных заводов JBS от дальнейшего сбоя и ограничения потенциального воздействия на рестораны, продуктовые магазины и фермеров, которые полагаются на JBS, сказал Андре Ногейра, исполнительный директор американского подразделения бразильской мясной компании JBS SA.

«Было очень больно платить преступникам, но мы поступили правильно для наших клиентов», – сказал г-н Ногейра в среду в интервью The Wall Street Journal. Он добавил, что оплата была произведена после того, как большинство заводов JBS снова заработали.

JBS – крупнейшая в мире мясная компания по продажам, переработке говядины, птицы и свинины от Австралии до Южной Америки и Европы. В США компания является крупнейшим переработчиком говядины и основным поставщиком курицы и свинины. Его дочерняя компания Pilgrim's Pride Corp. PPC0,65%, также пострадавший от атаки, является вторым по величине переработчиком птицы в США после Tyson Foods Inc.

Атака на JBS была частью волны вторжений с использованием программ-вымогателей, когда компании предъявляют требования о многомиллионных платежах, чтобы восстановить контроль над своими операционными системами. Оператор трубопровода, по которому бензин доставляется в районы Восточного побережья, в мае заплатил около 4,4 миллиона долларов, чтобы восстановить контроль над его операциями и восстановить работу. Атаки показывают, как хакеры перешли от атак к компаниям с большим объемом данных, таким как розничные торговцы, банки и страховые компании, к поставщикам основных услуг, таким как больницы, транспортные операторы и пищевые компании.

Г-н Ногейра сказал, что JBS узнал об атаке рано утром в воскресенье, 30 мая, когда технический персонал заметил нарушения в работе некоторых серверов. Вскоре они обнаружили сообщение с требованием выкупа за восстановление доступа к системе компании. Г-н Ногейра, который путешествовал, сказал, что его разбудили около 5 часов утра, когда его главный финансовый директор позвонил ему и уведомил о вторжении.

JBS немедленно уведомил Федеральное бюро расследований, сказал г-н Ногейра, и технологическая группа компании начала отключать системы поставщика мяса, чтобы замедлить продвижение атаки. JBS обратился к поставщикам технологий, которые ранее работали с компанией, а также к экспертам и консультантам по кибербезопасности, которые начали переговоры с злоумышленниками.

На прошлой неделе ФБР приписало атаку JBS преступной банде вымогателей REvil. Г-н Ногейра сказал, что JBS и сторонние фирмы проводят криминалистический анализ его систем информационных технологий, и что пока не ясно, как злоумышленники получили доступ к системам JBS.

По словам г-на Ногейры, JBS поддерживает вторичные резервные копии всех своих данных, которые зашифрованы. Компания вернула работу на свои заводы его словам, используя эти системы резервного копирования. Он добавил, что пока компания добивалась хороших результатов, технологические эксперты JBS предупредили компанию, что нет никакой гарантии, что хакеры не найдут другого способа нанести удар, и консультанты JBS продолжили переговоры с злоумышленниками. Г-н Ногейра сказал, что компания уверена, что данные о клиентах, поставщиках или сотрудниках не были скомпрометированы в результате атаки, на основании проведенного ею криминалистического анализа.

«Мы не думали, что можем пойти на такой риск, что что-то может пойти не так в нашем процессе восстановления», – сказал г-н Ногейра о решении заплатить злоумышленникам. «Это была страховка для защиты наших клиентов».

Он сказал, что внешние консультанты JBS согласовывали сумму платежа с злоумышленниками и что компания информировала федеральных правоохранительных органов на протяжении всего процесса. Г-н Ногейра отказался указать, когда JBS произвел платеж, а также назвать экспертов по кибербезопасности.

ФБР официально отговаривает компании, пострадавшие от атак программ-вымогателей, платить хакерам, утверждая, что это поддерживает бурно развивающуюся преступную индустрию и что часто инструменты дешифрования, предоставляемые в обмен на выкуп, не работают.

Но высокопоставленные чиновники в администрации Байдена в последние недели заявили, что они признают, что решение является трудным для компаний, и в целом избегают осуждать эту практику. Однако в воскресенье министр энергетики Дженнифер Гранхольм заявила на канале NBC «Знакомьтесь, с прессой», что она поддержит закон, запрещающий компаниям платить такой выкуп. «Я не знаю, сейчас Конгресс или президент», – добавила она.

Некоторые законодатели заявили, что хотят рассмотреть вопрос о запрете платежей, одновременно выступая за требование, чтобы компании хотя бы раскрывали их.

Джозеф Блаунт, генеральный директор Colonial Pipeline, в среду выступил в защиту своего решения заплатить выкуп хакерам во время дачи показаний в Конгрессе. Он сказал законодателям, что не уверен, распространится ли взлом, повлиявший на бизнес-сеть компании, на операционную сеть, которая контролировала трубопровод.

«ФБР никогда не рекомендовало нам не платить», – сказал г-н Блаунт, описывая разговоры, которые имели место после того, как взлом был обнаружен, но пока трубопровод был отключен. Г-н Блаунт сказал, что компания в конечном итоге полагалась на резервные копии для восстановления своих систем, но сказал, что неуплата могла замедлить процесс восстановления.

«Подумайте, как бы мы выглядели, если бы не возобновили работу трубопровода до следующей недели», – сказал он». ***(Jacob Bunge. JBS Paid $11 Million to Resolve Ransomware Attack // Dow Jones & Company, Inc. (https://www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781?mod=mhp). 09.06.2021).***

***

**«Программы-вымогатели были главной темой обсуждения президента США Джо Байдена и президента России Владимира Путина во время их первого личного саммита в среду. После трехчасовой встречи в Женеве, Швейцария, оба лидера провели отдельные пресс-конференции, на которых намекнули на ключевые моменты обсуждения и потенциальный компромисс.**

Путин отрицал, что Россия укрывает группы программ-вымогателей, и отказался отвечать на вопросы о других кибератаках. Байден также не был уверен в том, что было согласовано между двумя лидерами, но подтвердил, что он давил на Путина конкретно по вопросу о программах-вымогателях.

«Я говорил о предложении, что определенная критическая инфраструктура должна быть закрыта для атак. Период. Кибер или любыми другими средствами. Я дал им список, 16 конкретных объектов. 16 определены как критическая инфраструктура», – сказал Байден.

Том Келлерманн, член Консультативного совета по кибер-расследованиям секретной службы США, сказал, что 16 организаций, о которых говорил Байден, были тем, что CISA определило как «критически важные секторы инфраструктуры».

Келлерманн добавил, что это 16 секторов: химическая промышленность, коммерческие предприятия, связь, критическое производство, плотины, оборонная промышленная база, чрезвычайная ситуация, энергетика, финансовые услуги, продовольствие и сельское хозяйство, государственные учреждения, здравоохранение и общественное здравоохранение, информационные технологии, ядерные реакторы, материалы и отходы, транспортные системы, водные и сточные системы.

Все эти сектора столкнулись с десятками атак с использованием программ-вымогателей за последние три года, и Байден сказал, что он подтолкнул Путина к пониманию того, через что проходят США. Он сослался на атаку программ-вымогателей на Colonial Pipeline, из-за которой некоторые части Восточного побережья в течение нескольких дней боролись за газ.

«Я посмотрел на него и спросил: «Что бы вы почувствовали, если бы вымогатели захватили трубопроводы с ваших нефтяных месторождений?» Он сказал: «Это будет иметь значение». Я указал ему, что у нас есть значительный кибер-потенциал. И он это знает», – сказал Байден журналистам.

Далее он сказал, что кибератаки из России имели "репутационные" последствия, о которых Путин знал.

Встреча последовала за строгим предупреждением, которое было направлено США и другими странами G7 в понедельник, в котором конкретно призвали Россию либо начать собственные кибератаки, либо укрыть организации, занимающиеся вымогательством.

G7 заявил, что России нужна, чтобы «определить, сорвать, и привлечь к ответственности тех, в пределах своих границ, которые ведут вымогатель атаку, злоупотребляющую виртуальную валюту для желобов выкупов и других киберпреступлений.»

НАТО также разослало заявление после саммита в Брюсселе, в котором подтверждается идея о том, что «воздействие значительных злонамеренных кумулятивных действий в киберпространстве при определенных обстоятельствах может рассматриваться как вооруженное нападение».

Келлерманн, который также возглавляет стратегию кибербезопасности в VMware, сказал, что саммит был «знаменательным моментом для цивилизации киберпространства», и похвалил Байдена за то, что он подчеркнул необходимость защиты важнейших отраслей.

«В результате такого разграничения я считаю, что количество атак с использованием программ-вымогателей на основные критически важные инфраструктуры сейчас уменьшится, но, возможно, они увеличатся против традиционных корпораций, например, в розничном и финансовом секторах».

Многие эксперты по кибербезопасности заявили, что саммит мало повлияет на группы программ-вымогателей, которым разрешено действовать безнаказанно в ряде стран.

Но идея о том, что кибербезопасность достигла уровня, достойного упоминания двумя мировыми лидерами, была для некоторых положительным знаком.

«Это было отличное использование «трибуны хулиганов», чтобы дать миру понять, что кибербезопасность важна для Америки – и в особенности для офиса президента. У нас в мире кибербезопасности уже есть менталитет «все руки на палубе» – но приятно видеть, что наша озабоченность теперь разделяется через призму лидерства за пределами нашего сектора, – сказал генеральный директор YouAttest Гаррет Граек.

Елена Элькина, партнер консалтинговой фирмы Aleada по вопросам конфиденциальности и защиты данных, отметила, что Путину не нравятся

требования или ему говорят, что делать. Она предсказывала, что он более сдержанно отреагирует на убедительные заявления Байдена о кибератаках. «Это будет что-то более осязаемое, что сделает очевидным его мнение», – сказала она.

Исследователь кибербезопасности Хлоя Мессдаги сказала, что саммит был лишь одним из проявлений более глубокой «кибер-холодной войны», от которой обеим странам необходимо отказаться. Хотя саммит стал хорошим началом для решения проблем между обеими странами, Мессдаги сказал, что будет трудно заключить официально оформленные пакты о кибербезопасности.

«Реальность такова, что у нас, возможно, никогда не будет абсолютных и эффективных договоренностей на уровне договоров о кибератаках, потому что так много делается по доверенности, но каждая глобальная сверхдержава должна стремиться предотвратить хаос в своих границах», – добавил Мессдаги». ***(Jonathan Greig. Biden and Putin spar over cybersecurity, ransomware at Geneva summit // ZDNet (https://www.zdnet.com/article/biden-and-putin-spar-over-cybersecurity-ransomware-at-geneva-summit/). 17.06.2021).***

***

**«Более половины организаций заплатят выкуп, если станут жертвами атаки вымогателя, несмотря на неоднократные предупреждения о том, что они не должны поощрять киберпреступное вымогательство.**

Исследование, проведенное Советом международной безопасности Neustar (NISC), показало, что шесть из десяти организаций будут платить киберпреступникам за ключ дешифрования в случае атаки программы-вымогателя, согласно опросу 300 сотрудников, занимающих «руководящие должности».

Это, несмотря на подобный The White House, Министерство внутренних дел Великобритании, правоохранительные и кибербезопасность эксперты предупреждают, что платить выкуп следует избегать, поскольку она сигнализирует вымогатель операций, их схема вымогательства работы.

Среди известных жертв атак программ-вымогателей, недавно заплативших выкуп, можно назвать Colonial Pipeline, которая заплатила более 4 миллионов долларов в биткойнах киберпреступникам, использующим вымогатель DarkSide, а мясоперерабатывающий завод JBS заплатил 11 миллионов долларов в биткойнах преступникам, которые скомпрометировали его сеть с помощью вымогателя REvil.

Эти инциденты, по-видимому, заставили бизнес обратить на это внимание: 80% профессионалов в области кибербезопасности, опрошенных в ходе исследования, заявили, что больше внимания уделяется защите от угроз программ-вымогателей.

Однако четверть респондентов опасаются, что их текущие процедуры безопасности могут не обеспечить полную защиту от угроз программ-вымогателей, называя их «в некоторой степени» или «очень» недостаточными.

Когда дело доходит до программ-вымогателей, лучшее, что может сделать организация, – это в первую очередь предотвратить их превращение в проблему. Процедуры кибербезопасности, такие как применение многофакторной аутентификации в сети, своевременное применение исправлений безопасности для защиты от известных уязвимостей и регулярное обновление резервных копий и их

хранение в автономном режиме, могут помочь организациям предотвратить их нарушение в результате атаки программ-вымогателей.

Применение такого рода средств защиты снижает вероятность того, что организации почувствуют необходимость уступить требованиям вымогательства со стороны киберпреступников.

«Компании должны объединиться, чтобы не платить выкуп. Злоумышленники будут продолжать увеличивать свои требования о еще больших суммах выкупа, особенно если они увидят, что компании готовы платить. Эту спираль вверх необходимо остановить», – сказал Родни Джоффе, председатель NISC и сотрудник компании. Neustar». ***(Danny Palmer. Ransomware: Too many firms are still willing to pay up if attacked // ZDNet (https://www.zdnet.com/article/ransomware-too-many-firms-are-still-willing-to-pay-up-if-attacked/). 17.06.2021).***

***

**«Исследователи подробно рассмотрели, как работает LockBit, одна из новейших групп программ-вымогателей.**

В этом году программы-вымогатели стали одной из самых разрушительных форм кибератак. Еще в 2017 году, когда произошла глобальная вспышка WannaCry, мы впервые увидели серьезные нарушения, которые могло вызвать вредоносное ПО, и в 2021 году, похоже, ничего не изменилось к лучшему.

Только в этом году мы наблюдали катастрофу с использованием программы-вымогателя Colonial Pipeline, которая привела к нехватке топлива в некоторых частях США; продолжающиеся проблемы в национальной службе здравоохранения Ирландии и систематические сбои в работе гиганта мясопереработки JBS из-за вредоносного ПО.

Операторы программ-вымогателей будут развертывать вредоносные программы, способные шифровать и блокировать системы, а также могут украсть конфиденциальные данные во время атаки. Затем требуется оплата за ключ дешифрования.

Теряя деньги за секунду, пока их системы не реагируют, игроки-жертвы предприятий могут быть подвергнуты второму залпу, призванному нарастить давление – угроза утечки корпоративных данных или их продажи в Интернете через так называемые сайты утечки в темная паутина.

По прогнозам Cybersecurity Ventures, к 2031 году атаки программ-вымогателей во всем мире обойдутся в 265 миллиардов долларов, а выплаты в настоящее время обычно достигают миллионов долларов, как, например, в случае с JBS. Однако нет гарантии, что ключи дешифрования подходят для данной цели или что однократная оплата означает, что организация больше не пострадает.

Опрос Cybereason, опубликованный на этой неделе, показал, что до 80% предприятий, которые стали жертвами программ-вымогателей и заплатили, испытали вторую атаку – возможно, со стороны тех же злоумышленников.

Угроза программ-вымогателей для предприятий и важнейших коммунальных предприятий стала настолько серьезной, что этот вопрос был поднят во время

встречи президента США Джо Байдена и президента России Владимира Путина на саммите в Женеве.

У каждой группы свои методы работы, и операторы программ-вымогателей постоянно «уходят на пенсию» или присоединяются к группе, часто через партнерскую модель «Программа-вымогатель как услуга» (RaaS).

В пятницу группа Prodaft Threat Intelligence (PTI) опубликовала отчет (.PDF) о LockBit и его филиалах.

Согласно исследованию, LockBit, ранее работавший под названием ABCD, управляет структурой RaaS, которая предоставляет аффилированным группам центральную панель управления для создания новых образцов LockBit, управления их жертвами, публикации сообщений в блогах, а также получения статистики, касающейся успех – или неудача – их попыток атаки.

Расследование показало, что филиалы LockBit чаще всего покупают доступ к серверам по протоколу удаленного рабочего стола (RDP) в качестве первоначального вектора атаки, хотя они также могут использовать типичные методы фишинга и заполнения учетных данных.

«Такие виды специализированных услуг доступа можно приобрести всего за 5 долларов, что делает такой подход очень прибыльным для аффилированных лиц», – отмечает Продафт.

Эксплойты также используются для компрометации уязвимых систем, включая уязвимости Fortinet VPN, которые не были исправлены на целевых машинах.

Криминалистические исследования машин, атакованных филиалами LockBit, показывают, что группы угроз часто сначала пытаются идентифицировать «критически важные» системы, включая устройства NAS, серверы резервного копирования и контроллеры домена. Затем начинается кража данных, и пакеты обычно загружаются в службы, включая платформу облачного хранения MEGA.

Затем образец LockBit развертывается вручную, и файлы шифруются с помощью сгенерированного ключа AES. Резервные копии удаляются, а системные обои заменяются запиской о выкупе, содержащей ссылку на адрес веб-сайта.onion для покупки программного обеспечения для дешифрования.

Веб-сайт также предлагает «пробную» расшифровку, в которой один файл размером менее 256 КБ может быть расшифрован бесплатно.

Однако это не только для того, чтобы показать, что расшифровка возможна. Зашифрованный файл необходимо отправить аффилированным лицам для создания дешифратора для этой конкретной жертвы.

Если жертвы обращаются к ним, злоумышленники могут открыть окно чата на панели LockBit, чтобы поговорить с ними. Разговоры часто начинаются с требования выкупа, срока платежа, метода – обычно в биткойнах (BTC) – и инструкций о том, как купить криптовалюту.

Prodaft смог получить доступ к панели LockBit, в которой были указаны имена пользователей аффилированных лиц, количество жертв, даты регистрации и контактные данные.

Исследовательская группа говорит, что подсказки в названиях и адресах филиалов предполагают, что некоторые из них также могут быть зарегистрированы в Babuk и REvil, двух других группах RaaS, однако расследование продолжается.

В среднем филиалы LockBit запрашивают примерно 85 000 долларов с каждой жертвы, 10–30% из которых достаются операторам RaaS, а программа-вымогатель заразила тысячи устройств по всему миру. Более 20% жертв на дашборде были из сектора программного обеспечения и услуг.

«Группа LockBit также сильно нацелена на коммерческие и профессиональные услуги, а также транспортный сектор», – говорит Продафт. «Однако следует отметить, что размер выкупа определяется партнером после различных проверок с использованием онлайн-сервисов. Эта сумма зависит не только от сектора жертвы»…». ***(Charlie Osborne. A deep dive into the operations of the LockBit ransomware group // ZDNet (https://www.zdnet.com/article/a-deep-dive-into-the-operations-of-the-lockbit-ransomware-group/). 18.06.2021).***

***

**«Большинство предприятий, которые предпочитают платить за восстановление доступа к своим зашифрованным системам, подвергаются последующей атаке со стороны программ-вымогателей.** И почти половина из тех, кто платит, говорят, что некоторые или все их данные были повреждены.

Около 80% организаций, потребовавших выкуп, испытали вторую атаку, из которых 46% полагали, что последующие программы-вымогатели были вызваны теми же хакерами. Согласно опросу Cybereason, опубликованному в среду, среди тех, кто заплатил за восстановление доступа к своим системам, 46% заявили, что по крайней мере часть их данных была повреждена. В исследовании, проведенном Censuswide, приняли участие 1263 специалиста по безопасности на семи рынках по всему миру, в том числе 100 в Сингапуре, а также респонденты из Германии, Франции, США и Великобритании.

Во всем мире 51% восстановили свои зашифрованные системы без потери данных, в то время как 3% заявили, что не восстановили доступ к каким-либо зашифрованным данным. В отчете говорится, что одна конкретная организация, как сообщается, заплатила за программу-вымогатель миллионы долларов только для того, чтобы стать мишенью для второй атаки тех же злоумышленников в течение двух недель.

В Сингапуре 90% подверглись второй атаке программы-вымогателя после уплаты первого выкупа, а 28% восстановили доступ к поврежденным данным. Около 73% признали, что они потеряли доход в результате атаки, по сравнению со средним глобальным показателем 66%, в то время как 40% заметили, что их бренд или репутация пострадали, по сравнению с 53% в мире.

Около 37% сингапурских организаций, которые заплатили вымогателям, разделили от 140 000 до 1,4 миллиона долларов, а 5% заплатили выкуп в размере не менее 1,4 миллиона долларов. Еще 13% признали, что им пришлось уволить сотрудников из-за финансовых потерь после атаки, а 20% были вынуждены закрыться.

Вице-президент Cybereason по Азиатско-Тихоокеанскому региону Лесли Вонг сказал: «Сингапурские компании должны понимать, что уплата выкупа не гарантирует успешного восстановления, не мешает злоумышленникам снова нанести удар по организации-жертве и, в конце концов, только усугубляет проблему, поощряя еще больше. Если вы столкнетесь с угрозой, приняв стратегию предотвращения в первую очередь для раннего обнаружения, это позволит организациям остановить вредоносные программы-вымогатели до того, как они нанесут ущерб бизнесу».

В глобальном масштабе исследование показало, что 81% респондентов серьезно обеспокоены рисками, связанными с такими атаками, при этом 73% заявили, что у них есть политика или планы, специально предназначенные для управления атаками программ-вымогателей.

Вымогатели атаки по прогнозам, стоимость 265 $ млрд по всему миру в 2031, с одной атаки, воздействующие предприятиями и потребителями каждые несколько секунд, по кибербезопасности Ventures. В этом году стоимость таких атак оценивалась в 20 миллиардов долларов, что в 57 раз больше, чем в 2015 году.

Check Point Research также показала в среду, что среднее количество атак программ-вымогателей во всем мире выросло на 20% за последние два месяца, на 41% за последние шесть месяцев и 93% за последний год.

В Сингапуре количество таких атак выросло на 40% за последние пару месяцев, 99% за последние полгода и 147% за последний год, сообщил поставщик средств защиты. Он добавил, что в Латинской Америке и Европе наблюдался самый высокий всплеск атак программ-вымогателей с начала 2021 года – 62% и 59% соответственно.

Опрос Veritas в ноябре прошлого года показал, что 78% предприятий в Сингапуре и 88% в Австралии выплатили выкуп полностью или частично после того, как стали жертвами таких атак. Кроме того, 45% в Сингапуре потребовалось от пяти до 10 дней для полного восстановления после атаки вымогателя, по сравнению с 11% в Индии и 35% в Китае.

Поставщики кибербезопасности обычно советуют организациям не платить после атаки программ-вымогателей, вместо этого рекомендуя предприятиям принять стратегию защиты и восстановления данных.

Cybereason, однако, отметила, что планы резервного копирования данных не будут работать так же эффективно, когда киберпреступники запустят атаки вредоносного ПО с «двойным вымогательством», в которых хакеры выходят за рамки шифрования данных для кражи конфиденциальных данных и интеллектуальной собственности. Затем они угрожали раскрыть или продать украденные данные, если их требования о выкупе не будут выполнены». ***(Eileen Yu. Most firms face second ransomware attack after paying off first // ZDNet (https://www.zdnet.com/article/most-firms-face-second-ransomware-attack-after-paying-off-first/). 16.06.2021).***

***

**«Программы-вымогатели – одна из ключевых угроз кибербезопасности, с которыми сталкивается Великобритания, и киберпреступные группы,**

**стоящие за ними, становятся все более опасными, предупреждает кибер-глава Великобритании.**

Линди Кэмерон, глава Национального центра кибербезопасности (NCSC), скажет, что организация – подразделение по кибербезопасности шпионского агентства GCHQ – привержена борьбе с угрозой программ-вымогателей и «ежедневно поддерживает жертв программ-вымогателей», но это скоординированная ответ необходим для борьбы с растущей угрозой.

В то время как спонсируемые государством хакерские кампании представляют собой «злонамеренную стратегическую угрозу национальным интересам Великобритании», именно киберпреступность – и, в частности, программы– вымогатели – стали самой большой угрозой.

«Для подавляющего большинства граждан и предприятий Великобритании, а также для подавляющего большинства поставщиков критически важной национальной инфраструктуры и поставщиков государственных услуг, основная ключевая угроза – не государственные субъекты, а киберпреступники», – должен сказать Кэмерон в своем выступлении перед Исследовательский центр по вопросам обороны и безопасности Королевского института объединенных служб (RUSI).

Недавние инциденты, такие как атаки программ-вымогателей на Colonial Pipeline и мясоперерабатывающий завод JBS, а также атаки программ–вымогателей на ирландскую службу здравоохранения, продемонстрировали, насколько разрушительными могут быть эти киберпреступные кампании для критически важных служб.

Между тем, британские организации, включая предприятия, государственные учреждения, школы и университеты, в этом году стали жертвами атак программ-вымогателей.

Киберпреступные группы программ-вымогателей не только шифруют сети и требуют значительного платежа в обмен на ключ дешифрования, теперь они также часто крадут конфиденциальную информацию и угрожают выпустить ее, если не будет уплачен выкуп, что часто приводит к тому, что жертвы чувствуют себя так, как будто у них нет другого выбора, кроме как уступить требованиям вымогательства.

«По мере того, как бизнес-модель становится все более и более успешной, когда эти группы получают значительные суммы выкупа от крупных прибыльных предприятий, которые не могут позволить себе потерять свои данные из-за шифрования или потерять время простоя, пока их услуги отключены, рынок программ-вымогателей стал становится все более профессиональным», – скажет Кэмерон.

Программа-вымогатель успешна, потому что она работает; во многих случаях, потому что организации до сих пор не имеют соответствующей киберзащиты для предотвращения проникновения киберпреступников в их сеть, в первую очередь, что генеральный директор NCSC описывает как «совокупный эффект неспособности управлять киберрисками и неспособности серьезно относиться к угрозе киберпреступности».

Но еще одна причина, по которой это стало такой проблемой, особенно для Запада, заключается в том, что многие из наиболее успешных групп программ-

вымогателей работают в том, что Кэмерон описывает как «заграничные юрисдикции, которые закрывают глаза или иным образом не действуют для преследования этих групп».

В частности, считается, что Россия является домом для ряда киберпреступных группировок вымогателей, но правительство не вмешивается в их деятельность, потому что они не наносят вреда российскому бизнесу или гражданам.

«Эти преступники существуют не в вакууме. Часто им помогают и содействуют безнаказанно действующие государства», – сказала она.

Однако Кэмерон скажет, что бороться с вирусом программ-вымогателей можно, объединив усилия экспертов по кибербезопасности, правительства и используя более широкое международное сотрудничество.

«В некоторых отношениях наш ответ на программы-вымогатели прост: мы должны продолжать повышать киберустойчивость Великобритании, чтобы атаки не могли достичь своих целей», – сказала она.

«Но во многих других отношениях это требует реакции всего правительства. Это начинается с усилий по предотвращению деятельности групп, стоящих за этими разрушительными атаками».

Однако программы-вымогатели представляют собой проблему не только для Великобритании, и Кэмерон подчеркнул важность сотрудничества с другими странами для решения действительно международной проблемы». ***(Danny Palmer. Ransomware is the top cybersecurity threat we face, warns cyber chief // ZDNet (https://www.zdnet.com/article/ransomware-is-the-key-online-cybersecurity-threat-to-people-and-businesses-warns-cyber-chief/). 143.06.2021).***

***

**«Число атак программ-вымогателей, нацеленных на школы, колледжи и университеты, снова растет, предупреждает Национальный центр кибербезопасности Великобритании (NCSC)…**

NCSC ранее предупреждал об атаках программ-вымогателей, нацеленных на сектор образования, но в конце мая – начале июня произошло еще одно увеличение инцидентов – в критическое время года, когда дело касается курсовых работ, экзаменов и других заданий.

NCSC ранее подробно рассказывал, как инциденты с программами-вымогателями, влияющие на образование, привели к потере студентами курсовой работы, финансовой отчетности школы, а также данных, относящихся к тестированию на COVID-19.

«Важно, чтобы высшее руководство понимало природу угрозы и потенциальную возможность того, что программы-вымогатели нанесут значительный ущерб их учреждениям с точки зрения потери данных и доступа к критически важным службам», – говорится в предупреждении NCSC.

Некоторые из наиболее распространенных методов, которые киберпреступники используют для получения доступа к университетским сетям и создания основы для атак программ-вымогателей, включают нацеливание на протокол удаленного рабочего стола (RDP) и виртуальные частные сети (VPN).

Используя слабые пароли, отсутствие многофакторной аутентификации или незащищенные уязвимости в RDP и VPN, киберпреступники могут незаметно взламывать сети. Их присутствие часто обнаруживается только после того, как они начали атаку программ-вымогателей и зашифровали системы и службы.

Чтобы помочь предотвратить атаки программ-вымогателей, NCSC рекомендует организациям иметь эффективные процедуры управления уязвимостями и исправлений, чтобы они могли быстро обновлять сети и программное обеспечение с помощью соответствующих исправлений безопасности при появлении новых уязвимостей.

NCSC также предлагает, чтобы RDP и другие облачные сервисы были защищены с помощью многофакторной аутентификации и чтобы были внедрены механизмы, помогающие обнаруживать и предотвращать фишинговые атаки.

Также рекомендуется, чтобы организации в секторе образования – и за его пределами – имели планы по обеспечению эффективного восстановления, поэтому, если произойдет худшее, и сеть будет зашифрована с помощью программы-вымогателя, ее можно будет восстановить, не уступая требованиям выкупа со стороны киберпреступников.

Это может быть достигнуто за счет наличия обновленных и протестированных автономных резервных копий, поскольку, согласно NCSC, «автономные резервные копии являются наиболее эффективным способом восстановления после атаки программ-вымогателей». ***(Danny Palmer. Ransomware warning: There's been another spike in attacks on schools and universities // ZDNet (https://www.zdnet.com/article/ransomware-warning-theres-been-another-spike-in-attacks-on-schools-and-universities/). 07.06.2021).***

***

**«Исследователи представили тематическое исследование Nefilim, оператора программы-вымогателя, который использует тактику «двойного вымогательства» для обеспечения оплаты от организаций-жертв.**

Программы-вымогатели – это разновидность вредоносного ПО, которое создается для шифрования скомпрометированных систем. Как только он попадает на уязвимую машину – будь то фишинговое сообщение, уязвимость программного обеспечения, украденные учетные данные или другие средства – файлы и диски будут зашифрованы и могут быть восстановлены только с помощью ключа дешифрования.

Ключ дешифрования – это пряник, который болтается перед жертвами, которым обычно обещают ключ и средства для восстановления их систем за плату. Когда дело доходит до корпоративных игроков, требования выкупа могут достигать миллионов долларов – и никогда нет гарантии, что ключ будет выпущен или будет технически пригоден для восстановления.

Фраза «программы-вымогатели» стала привычной для широкой публики, поскольку еженедельно мы слышим о новых случаях.

В последние месяцы на Colonial Pipeline произошла вспышка программы-вымогателя, которая в конечном итоге привела к нехватке топлива в некоторых

частях Соединенных Штатов, а после заражения национальной службы здравоохранения Ирландии HSE по-прежнему испытывает «серьезные» нарушения.

Что отличает программы-вымогатели, так это возможность «двойного вымогательства» – относительно новая тактика, призванная усилить давление на жертв с целью их выплаты. Во время кибератаки операторы программ-вымогателей, включая Maze, Nefilim, REvil и Clops, крадут конфиденциальные данные и угрожают опубликовать или продать эту информацию на веб-сайте утечки.

Во вторник компания Trend Micro опубликовала тематическое исследование Nefilim, группы программ-вымогателей, которая, по мнению исследователей, изначально связана или была связана с Nemty как программа-вымогатель как услуга (RaaS).

Nemty появился на сцене в 2019 году, но вместе с Sentinel Labs Trend Micro сообщает, что Nefilim возник в марте 2020 года.

Оба участника, которых фирма называет «Water Roc», предлагали услуги подписки RaaS на основе разделения 70/30 с прибылью, сниженной до 90/10, когда высокопоставленные жертвы были пойманы филиалами.

Trend Micro сообщает, что Nefilim часто сосредотачивается на открытых службах удаленных рабочих столов (RDP) и общедоступном тестовом коде (PoC) для обнаружения уязвимостей. К ним относятся CVE-2019-19781 и CVE-2019-11634, обе из которых являются известными ошибками в шлюзах Citrix, которые получили исправления в 2020 году.

Однако при обнаружении неустановленных сервисов запускается код эксплойта и получается начальный доступ. Nefilim начинает с загрузки маяка Cobalt Strike, Process Hacker, используемого для отключения агентов безопасности конечных точек, дампера учетных данных Mimikatz и дополнительных инструментов.

В одном случае, задокументированном командой, Nefilim также смог воспользоваться CVE-2017-0213, старой уязвимостью в программном обеспечении компонентной объектной модели Windows (COM). Хотя исправление было выпущено еще в 2017 году, ошибка все еще присутствовала и позволила группе повысить свои привилегии до уровня администратора.

Операторы программ-вымогателей также могут использовать украденные или легко взломанные учетные данные для доступа к корпоративным сетям и для горизонтального перемещения.

MEGAsync может использоваться для кражи данных во время атак. Затем будет развернута программа-вымогатель Nefilim, которая начнет шифрование контента. Расширения различаются, но группа связана с расширениями.Nephilim, Merin и.Off-White.

Для каждого файла, поставленного в очередь на шифрование, генерируется случайный ключ AES. Затем вредоносная программа расшифрует записку о выкупе с помощью фиксированного ключа RC4, который предоставляет жертвам адреса электронной почты, чтобы связаться с ними по поводу оплаты.

«Чтобы включить дешифрование файла в случае, если жертва заплатит сумму выкупа, вредоносная программа шифрует сгенерированный ключ AES с

фиксированным открытым ключом RSA и добавляет его в зашифрованный файл», – говорят исследователи. «На сегодняшний день только злоумышленники могут расшифровать эту схему, поскольку только они владеют парным закрытым ключом RSA».

Что касается жертв, Nefilim чаще всего был связан с атаками на организации, приносящие годовой доход в 1 миллиард долларов и более; однако в прошлом операторы вредоносного ПО поражали и более мелкие компании.

Большинство жертв находятся в США, за которыми следуют Европа, Азия и Океания.

«Современные злоумышленники перешли от широко распространенных программ-вымогателей неизбирательной рассылки по почте к новой модели, которая является гораздо более опасной», – заявляет Trend Micro. «Сегодня корпорации подвергаются этим новым атакам программ-вымогателей уровня APT. На самом деле они могут быть хуже, чем APT, потому что программы-вымогатели часто заканчивают тем, что уничтожают данные, тогда как APT, похищающие информацию, почти никогда не являются разрушительными. Существует более острая необходимость в защите организации против атак программ-вымогателей, и теперь ставки намного выше». ***(Charlie Osborne. A deep dive into Nefilim, a ransomware group with an eye for $1bn+ revenue companies // ZDNet (https://www.zdnet.com/article/a-deep-dive-into-nefilim-a-double-extortion-ransomware-group/). 08.06.2021).***

***

**«Во вторник утром появилась новость о том, что iConstituent, платформа, созданная для облегчения общения между политиками и местными жителями, борется с атакой программ-вымогателей.**

iConstituent не ответила на запросы о комментариях, но Punchbowl News сообщили, что платформу используют почти 60 членов Конгресса. Главный административный директор Дома Кэтрин Шпиндор сообщила новостному агентству, что они были уведомлены об атаке программ-вымогателей на систему электронной рассылки iConstituent, доступ к которой члены палаты покупают.

Но Шпиндор добавил, что никакие данные из Дома не были получены или получены, и сеть, используемая Домом, не пострадала.

Старший советник Sophos по безопасности Джон Шиер сказал, что эта атака была еще одним примером того, как злоумышленники используют цепочки поставок для получения доступа к более крупным целям.

«Независимо от того, что вы делаете, вы находитесь в чьей-то цепочке поставок, предоставляете ли вы услуги напрямую другой стороне или являетесь частью более крупной организации или механизма, который предоставляет услуги или продукты другим людям», – сказал Шиер.

Платформа также широко используется правительствами штатов Невада, Джорджия, Гавайи и таких городах, как Лос-Анджелес. Ассамблея штата Нью-Йорк также имеет контракт с компанией на оказание услуг.

Атака была раскрыта, когда Белый дом и правоохранительные органы заняли более решительную позицию в отношении программ-вымогателей после

разрушительных атак на крупнейшего переработчика мяса в стране и одного из крупнейших поставщиков нефти и газа в стране.

Жесткая риторика мало что сделала, чтобы помешать киберпреступникам совершать самые разнообразные атаки на учреждения через правительства штатов и городов. В воскресенье был взломан юридический отдел Нью-Йорка, в результате которого ИТ-администраторы были вынуждены закрыть доступ к определенным системам для более чем 1000 сотрудников.

Организация занимается всеми правовыми вопросами города и хранит огромное количество личной информации о сотрудниках города, включая номера социального страхования, адреса и многое другое. Мэр Билл де Блазио выступил по телевидению и сказал, что не было запроса о выкупе или компрометации городских данных, но следователи все еще оценивают ситуацию.

Раджив Пимпласкар, директор по рискам Veridium, сказал ZDNet, что в Нью-Йорке есть одна из лучших в стране инфраструктур и организаций ИТ и кибербезопасности, продемонстрировав, что независимо от того, насколько вы хороши, никто не застрахован от взломов.

И Шиер, и Пимпласкар добавили, что правительственные учреждения являются зрелыми целями из-за того, сколько личной информации они несут, и потому, что они часто используют устаревшие системы и технологии.

«Отделы, которые занимаются конфиденциальной информацией и данными клиентов, являются основными целями для злоумышленников, поскольку они представляют собой ловушку для личной информации, которая может быть целью сама по себе или, в свою очередь, может быть использована для социальной инженерии и вторичных атак», – сказал Пимпласкар». ***(Jonathan Greig. Constituent platform used by Congress hit with ransomware as NYC faces legal department hack // ZDNet (https://www.zdnet.com/article/constituent-platform-used-by-congress-hit-with-ransomware-as-nyc-faces-legal-department-hack/). 08.06.2021).***

***

**«Служба здравоохранения Ирландии по-прежнему страдает от серьезных сбоев более чем через три недели после того, как стала жертвой атаки вымогателя.**

Управление здравоохранения (HSE), отвечающее за здравоохранение и социальные услуги в Ирландии, отключило все свои ИТ-системы после атаки в прошлом месяце.

Многие из этих систем были отключены в качестве «меры предосторожности», чтобы остановить распространение программы– вымогателя, которую HSE описал как вариант программы– вымогателя Conti.

Служба здравоохранения пообещала не платить выкуп, о котором сообщалось, как о требовании 20 миллионов долларов в биткойнах, а Высокий суд Дублина вынес судебный запрет против Конти, чтобы предотвратить утечку украденных данных преступниками за то, что им не заплатили.

HSE регулярно предоставляет обновления после кибератаки, и по состоянию на 3 июня – через три недели после первоначального инцидента – службы по всей

Ирландии продолжают сталкиваться с тем, что описывается как «значительные воздействия и сбои в работе служб».

Основные и срочные службы, включая вакцинацию от COVID-19, работают, но пациентов по-прежнему предупреждают, что они могут столкнуться с задержками и отменой приема на прием, потому что «системы не работают как обычно» из-за того, что «критические ИТ-системы» все еще не работают.

Такие службы, как анализы крови и диагностика, работают намного дольше, чем обычно, потому что продолжающиеся последствия заставляют врачей, медсестер и другой персонал в то же время полагаться на ручные процессы.

Согласно HSE, ожидается, что это продлится «несколько недель», поскольку будут предприняты усилия по безопасному развертыванию инструмента дешифрования для восстановления 2000 ИТ-систем, каждая из которых состоит из инфраструктуры, нескольких серверов и устройств, затронутых программой-вымогателем, на основе клинический приоритет.

Несмотря на попытку наложить судебный запрет, HSE предупредила общественность, что преступники могут попытаться воспользоваться путаницей и беспокойством по поводу безопасности своих медицинских данных, чтобы обманывать и обманывать людей.

«Людям, получающим подозрительные звонки, текстовые сообщения или другие контакты, которые хотят получить личные или банковские реквизиты, рекомендуется сообщать об этих контактах в местное отделение Гарда или на конфиденциальную линию Гарда 1800 666111», – говорится в заявлении HSE…» ***(Danny Palmer. Ransomware: Ireland's health service remains 'significantly' disrupted weeks after attack // ZDNet (https://www.zdnet.com/article/ransomware-irelands-health-service-is-still-significantly-disrupted-weeks-after-attack/). 04.06.2021).***

***

**«Ожидается, что стоимость инцидентов с программами-вымогателями во всем мире выйдет из-под контроля и к 2031 году превысит 265 миллиардов долларов.**

В настоящее время программы– вымогатели являются одним из наиболее потенциально опасных и очень популярных видов вредоносного ПО. Если вымогатель попадает в уязвимую систему, файлы обычно зашифровываются, пользователи блокируются, и требуется оплата, обычно в криптовалюте, в обмен на ключ дешифрования.

В более поздней эволюции приложений вымогателей операторы также будут красть информацию во время атаки и будут угрожать опубликовать эту информацию на сайтах утечки в темной сети или продать ее, что вдвое усиливает давление на жертв, чтобы они заплатили.

В настоящее время одними из самых известных групп, которые превратили программы-вымогатели в прибыльную «бизнес-возможность», являются Maze, Nefilim, Clop и DarkSide, последняя из которых покинула сцену – по крайней мере, под этим именем – после вымогательства у Colonial Pipeline из 4,4 миллиона долларов после разрушительной атаки, в результате которой были нарушены поставки топлива по Соединенным Штатам.

Cybersecurity Ventures прогнозирует, что ущерб, нанесенный программами-вымогателями, может обойтись мировой арене в 265 миллиардов долларов к 2031 году, исходя из того, что этот тип киберпреступности атакует как предприятия, так и потребителей со скоростью одна атака каждые несколько секунд.

В настоящее время агентство по кибербезопасности оценивает, что вымогатели обойдутся нам примерно в 20 миллиардов долларов в этом году, что в 57 раз больше, чем в 2015 году.

Последние оценки, опубликованные компанией, основаны на 30% -ном росте инцидентов в годовом исчислении.

Заражение программ-вымогателей может привести к дорогостоящим страховым взносам и выплатам, необходимости нанимать фирмы кибер-криминалистики для расследования инцидентов, ограничения ущерба или ремонта системы, потери данных и, возможно, платежей злоумышленникам для извлечения критических систем или предотвращения утечки данных.

Последняя оценка также включает нарушение бизнеса во время и после атаки, репутационный ущерб и расходы на обучение сотрудников после инцидента с программным вымогателем.

Palo Alto Networks предполагает, что только выплаты вымогателей выросли со 115 123 долларов в 2019 году до 312 493 долларов в 2020 году, что на 171% больше, чем в прошлом году. Самый большой спрос, зафиксированный в последние годы, составляет 30 миллионов долларов.

Несмотря на то, что правительственные чиновники со всего мира принимают участие в этом, в том числе такие фигуры, как президент США Байден, который недавно подписал указ, требующий от федеральных агентств работать над улучшением состояния кибербезопасности страны, инциденты с программами-вымогателями только усугубляются.

«Несмотря на недавний успех властей в пресечении нескольких банд вымогателей, именно эта разновидность вредоносных программ оказалась гидрой – отрубили одну голову, и на ее месте появилось несколько – и все признаки того, что грядущее десятилетие будет не менее проблемным», – отметили в Cybersecurity Ventures». ***(Charlie Osborne. The cost of ransomware attacks worldwide will go beyond $265 billion in the next decade // ZDNet (https://www.zdnet.com/article/the-cost-of-ransomware-around-the-globe-to-go-beyond-265-billion-in-the-next-decade/). 07.06.2021).***

***

**«В среду, 2 июня, заместитель советника по национальной безопасности по кибербезопасности и новым технологиям Энн Нойбергер опубликовала открытое письмо, в котором побудила предприятия частного сектора принять немедленные меры защиты от программ-вымогателей и других угроз кибербезопасности.** Рекомендации в письме полезны и подчеркивают общие уроки, извлеченные из растущей частоты и серьезности атак программ-вымогателей. Они также напоминают нам о необходимости постоянно оценивать риск сетевых угроз и внедрять комплексный подход к кибербезопасности для

снижения риска, включая развертывание усиленных мер безопасности для защиты от развивающихся вредоносных технологий.

Письмо Нойбергера следует после указа от 12 мая., который побудил государственных подрядчиков принять более строгие меры кибербезопасности и расширить сотрудничество с федеральными спецслужбами в ближайшие месяцы. Письмо от 2 июня, озаглавленное «Что мы призываем вас сделать для защиты от угрозы программ-вымогателей», призывает частные компании принять многие из тех же мер, которые будут применяться к федеральным подрядчикам в соответствии с указом президента. Предлагаемые политики можно разбить на три общих плана действий: резервное копирование, отдельное и безопасное.

Первое из предложений Нойбергера предусматривает использование пяти передовых методов из указа президента, каждый из которых был признан необходимым и эффективным для обнаружения атак программ-вымогателей и защиты от них:

реализовать многофакторную аутентификацию;

реализовать эвристические средства обнаружения конечных точек и реагирования;

реализовать шифрование для защиты данных, которые могут быть украдены;

привлекать квалифицированную команду безопасности для быстрого исправления и постоянного обновления мер безопасности; а также

делиться информацией об угрозах и использовать ее при создании защиты.

Второй набор предложений призывает к последовательному резервному копированию и шифрованию любой цифровой информации, хранящейся в бизнесе. Эти данные резервного копирования должны включать не только клиентские файлы или другую информацию о потребителе, но также системные образы и настройки. Любые оперативные данные, организационные или иные, должны иметь как минимум одну дополнительную зашифрованную копию. Компании должны регулярно тестировать эти резервные копии, чтобы гарантировать их работоспособность на случай, если файловые системы и данные потребуется восстановить после атаки программы-вымогателя. Эти данные резервного копирования и любые ресурсы цифровой компании в целом должны храниться отдельно. Хотя сетевые системы резервного копирования удобны, особенно для крупных корпоративных систем, Нойбергер отмечает, что атаки программ-вымогателей обычно нацелены и удаляют резервные копии, доступные из основной сети, оставляя предприятия без возможности восстановить скомпрометированные системы. Следовательно, в дополнение к сетевому резервному копированию бизнес должен гарантировать, что текущие резервные данные хранятся отдельно в автономном режиме, сохраняя возможность общесистемного восстановления в случае блокировки программы-вымогателя. В соответствии с этим следует учитывать правило резервного копирования 3-2-1. Это правило предусматривает, что у компании должно быть три копии своих данных – производственные данные и две резервные копии на двух разных носителях, причем одна копия должна быть удалена для аварийного восстановления.

Письмо от 2 июня также включает урок из недавних событий, таких как предупреждение 2 марта, касающееся уязвимостей Microsoft Exchange. В письме

компаниям рекомендуется незамедлительно обновлять и исправлять свои операционные системы, приложения, прошивки и другое связанное программное обеспечение. Эти общесистемные исправления и обновления обеспечивают самые современные функции безопасности и могут закрыть потенциальные лазейки, которые злоумышленники могут использовать для проникновения в бизнес-систему.

В письме также подчеркивается важность базового принципа информационной безопасности: сегментации сети. Например, сети, используемые для бизнес-функций, должны быть отделены от сетей, используемых для производства и производства. Таким образом, кибератака на одну сеть не повлияет на общую деятельность бизнеса, сохраняя статус-кво до тех пор, пока атака не будет устранена.

Наконец, общие предложения Нойбергера указывают на усиление внимания к безопасности с помощью локализованных групп реагирования на безопасность и стороннего тестирования уязвимостей. Помимо локального шифрования и стандартной защиты паролем, компаниям рекомендуется создавать собственные группы безопасности и разрабатывать планы реагирования на инциденты.

При формировании этих планов команды компании должны провести оценку рисков, чтобы определить, какие системы наиболее вероятно подвергнутся атаке, какая информация является наиболее важной для обычных бизнес-функций и как сохранить бизнес в рабочем состоянии в случае атаки с использованием программ-вымогателей. Команда Льюиса Брисбуа по защите данных и кибербезопасности имеет опыт работы с предприятиями для обеспечения максимальной безопасности данных и защиты от кибератак, включая разработку планов реагирования на инциденты и их тестирование с помощью настольных упражнений». ***(Brian Craig & George Leahy. BACKUP, SEPARATE, & SECURE: WHITE HOUSE CYBER RECOMMENDATIONS REACH THE PRIVATE SECTOR // Lewis Brisbois Bisgaard & Smith LLP (https://lewisbrisbois.com/blog/category/data-privacy-cyber-security/backup-separate-secure-white-house-cyber-recommendations-reach-the-private-sector). 07.06.2021).***

***

**«Саммит западных стран G7 призвал Россию «выявить, пресечь и привлечь к ответственности тех, кто в пределах ее границ проводит атаки с использованием программ-вымогателей, использует виртуальную валюту для отмывания выкупа и другие киберпреступления».**

Это заявление, сделанное после 18-месячного периода, когда банды вымогателей, действующие в основном из России и союзных с Россией стран, опустошали Запад, является частью растущей готовности противостоять бездействию России в отношении преступных группировок, базирующихся на ее территории.

В публичном коммюнике G7, выпущенном в минувшие выходные, когда политико-СМИ собрались вылететь домой с места проведения саммита в Корнуолле, говорилось, что «мы подтверждаем наш призыв к России прекратить свое дестабилизирующее поведение» и призываем остальной мир присоединиться к

более широким усилиям «срочно выявлять и разрушать преступные сети-вымогатели, действующие в пределах их границ, и привлекать эти сети к ответственности за их действия».

Недавние атаки программ-вымогателей (такие как захват REvil поставщика мяса JBS) исходили от банд, которые не нацелены на Россию. В преступном мире Интернета широко распространено мнение, что при условии, что вы не нацелены на Россию или ее союзников, российские правоохранительные органы не будут предпринимать никаких действий против вас.

Великобритания сообщает ООН, что национальные государства должны без предупреждения принимать ответные меры против кибер-злодеяния

JBS, производитель мяса с программ-вымогателем, признается, что заплатил 11 миллионов долларов за свою свободу

«Я ставлю интересы страны на первое место»: генеральный директор Colonial Pipeline о том, почему нефтяной бизнес расплачивался с мошенниками-вымогателями

Политика правды: что делать киберстраховщикам по мере роста числа заявлений о программах-вымогателях?

Британский ритейлер Furniture Village подтвердил "кибератаку", когда отключение систем началось с 7-го дня

Заявление G7 направлено на оказание давления на Владимира Путина с целью борьбы с угрозой программ-вымогателей, хотя стремление России к этому неясно. Как частные операторы, мешающие традиционным врагам России, банды вымогателей предоставляют полезные средства, которые нельзя отрицать, как вмешиваться в западные экономики и ключевые отрасли промышленности.

Профессор Алан Вудворд из Университета Суррея сказал The Register, что подход G7 мог бы принести плоды, если бы России дали достаточно большой пряник наряду с риторической палкой, предложенной в коммюнике: «Я видел записку, в которой Путин говорил, что он, возможно, рассматривает возможность передачи над некоторыми нападавшими (если окажется, что они находятся в России, чего, конечно, он не признает), если ему будут даны определенные гарантии».

Профессор добавил: «Я не удивлюсь, если на саммите Байдена и Путина [позднее на этой неделе] появится информация, позволяющая экстрадировать этих преступников. серьезно относиться к шуму из G7».

Министр иностранных дел США Энтони Блинкен сказал NBC News в воскресенье, что президент США Джо Байден будет противостоять Путину из-за кибератак, заявив телепрограмме: «[Байден] собирается дать понять, что ни одно ответственное государство не может заниматься укрывательством преступных предприятий. участвовал в кибератаках, в том числе с помощью программ-вымогателей. Это будет частью разговора ".

Коммюнике G7 также связывало страны, не входящие в альянс, вместе, чтобы «способствовать общему пониманию того, как существующее международное право применяется к киберпространству», – тема, которую Великобритания все чаще поднимает.

Энди Гарт, руководитель отдела по связям с правительством антивирусной компании ESET и бывший посол Великобритании в Словакии, прокомментировал: «Многостороннее сотрудничество в области кибербезопасности абсолютно необходимо. Киберпреступность достигла беспрецедентного уровня за последний год, и важно, чтобы единомышленники объединились. и коллективно стремиться лучше защитить граждан и нации от этого постоянно меняющегося ландшафта угроз».

Страны-участницы G7 – это Великобритания, США, Канада, Япония, Франция, Германия и Италия. Хотя все эти страны являются богатыми и западными по мировоззрению, если не обязательно по географическому положению, атаки программ-вымогателей влияют на них всех одинаково. Если G7 и саммит США / России позднее на этой неделе (начиная со среды, 16 июня) остановит приливную волну атак или приведет к заключению специального соглашения об экстрадиции для передачи преступников-вымогателей, это станет решающим моментом в истории информационной безопасности». ***(Gareth Corfield. G7 nations call out Russia for harbouring ransomware crims ahead of Biden-Putin powwow // The Register (https://www.theregister.com/2021/06/14/g7_ransomware_communique_calls_out_russia/). 14.06.2021).***

***

**«Японский многонациональный конгломерат Fujifilm заявляет, что он возобновил нормальный бизнес и операции с клиентами после атаки программы-вымогателя, которая вынудила его отключить всю сеть 4 июня.**

Примерно в 10 часов утра по восточному стандартному времени Fujifilm попросила сотрудников немедленно выключить свои компьютеры и все серверы в сети после того, как продолжающийся сбой сети заблокировал доступ к электронной почте, биллинговой системе и внутренней системе отчетности.

*Доказательств украденных данных пока нет*

«После этого, с 4 июня, мы начали эксплуатировать серверы и компьютеры, которые были подтверждены как безопасные, и возобновили связь в сети, которая была заблокирована», – говорится в заявлении Fujifilm, опубликованном ранее сегодня.

«Мы рады сообщить вам, что к сегодняшнему дню восстановлена нормальная работа клиентов и деловых партнеров, такая как прием запросов и заказов, а также отгрузка нашей продукции».

Хотя в большинстве атак с использованием программ-вымогателей злоумышленники также извлекают данные перед шифрованием систем жертв, Fujifilm заявила, что «проведенные на данный момент расследования не обнаружили никаких доказательств утечки информации во внешний мир».

«Кроме того, уже приняты меры противодействия этому несанкционированному доступу. Мы продолжим отслеживать и продолжать укреплять информационную безопасность», – добавили в Fujifilm.

Мы приносим глубокие извинения за причинение больших неудобств и беспокойства нашим клиентам и деловым партнерам. – Корпорация Fujifilm

*Атака программ-вымогателей*

Хотя Fujifilm не раскрыла название операции вымогателя, которая смогла проникнуть в ее сеть и остановить ее 4 июня, генеральный директор Advanced Intel Виталий Кремез сообщил BleepingComputer, что некоторые системы компании были заражены трояном Qbot в прошлом месяце.

«Сетевая инфекция, приписываемая QBot, автоматически приводит к рискам, связанным с будущими атаками программ-вымогателей», – сказал Кремез.

Операторы троянца Qbot имеют долгую историю работы с бандами вымогателей, обеспечивая им удаленный доступ к ранее зараженным сетям.

ProLock и Эгрегор вымогателей группы, как известно, сотрудничает с КДЦ в прошлом, но, после того, как эти операции закрыли, Revil это новая вымогателей банда, которая использует ботнет для получения доступа к сетям жертв.

Хотя на данный момент это всего лишь теории, мы достаточно скоро узнаем, кто стоял за атакой, поскольку, если данные были украдены в ходе атаки, они, вероятно, будут опубликованы на сайте утечки данных программ-вымогателей и использованы в качестве рычага, чтобы заставить Fujifilm заплатить выкуп…». ***(Sergiu Gatlan. Fujifilm resumes normal operations after ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fujifilm-resumes-normal-operations-after-ransomware-attack/). 14.06.2021).***

***

**«Полный исходный код Paradise Ransomware был опубликован на хакерском форуме, что позволяет любому потенциальному киберпреступнику разработать свою собственную индивидуальную операцию вымогателя.**

Выпущенная на хакерском форуме XSS ссылка на исходный код доступна только активным пользователям сайта, которые ранее ответили или отреагировали на другие сообщения на сайте.

Исследователь Security Joes Том Малка, который поделился исходным кодом с BleepingComputer, скомпилировал пакет и обнаружил, что он создает три исполняемых файла – построитель конфигурации вымогателя, шифровальщик и дешифратор.

По всему исходному коду разбросаны комментарии на русском языке, показанные выше, которые ясно демонстрируют родной язык разработчика.

Аффилированный с программой-вымогателем Paradise может использовать конструктор для настройки своей собственной версии программы-вымогателя, включив в нее настраиваемый сервер управления и контроля, зашифрованное расширение файла и контактный адрес электронной почты.

После создания настраиваемой программы-вымогателя партнерские организации могут распространять вредоносное ПО в своих кампаниях для целевых жертв.

*Добро пожаловать в рай*

Операция Paradise Ransomware впервые была запущена в сентябре 2017 года с помощью фишинговых писем, содержащих вредоносные вложения IQY, которые загружали и устанавливали программу-вымогатель.

Со временем было выпущено несколько версий вымогателя, причем начальные версии содержали недостатки, которые привели к выпуску дешифратора Paradise Ransomware.

Однако в новых версиях метод шифрования был переведен на RSA, что препятствовало бесплатному дешифрованию файлов.

Майкл Гиллеспи, создавший оригинальный дешифратор Paradise Ransomware, сказал BleepingComputer, что выпущенные версии Paradise включают:

Paradise – Нативная версия, в которой были недостатки, позволяющие дешифровать.

Paradise.NET – безопасная версия.NET, которая переключила алгоритмы шифрования на использование шифрования RSA.

Paradise B29 – «Командный» вариант, который шифрует только конец файла.

Гиллеспи сказал, что неясно, были ли все они разработаны одной и той же группой, поскольку все они циркулировали примерно в одно и то же время с тысячами различных расширений, поскольку злоумышленники стекались к растущему Ransomware-as-a-Service.

Судя по статистике представлений в ID Ransomware, Paradise Ransomware широко распространялся в период с сентября 2017 года по январь 2020 года, когда внезапно снизился до сегодняшнего дня, где его редко можно увидеть.

К сожалению, Гиллеспи сообщает BleepingComputer, что исходный код предназначен для безопасной версии Paradise Ransomware, которая использует шифрование RSA для шифрования файлов.

Используя этот исходный код, другие злоумышленники могут легко модифицировать его, чтобы выпустить собственную настроенную версию программы-вымогателя, что позволяет легко начать создание новой операции программы-вымогателя». ***(Lawrence Abrams. Paradise Ransomware source code released on a hacking forum // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/paradise-ransomware-source-code-released-on-a-hacking-forum/). 15.06.2021).***

***

**«В новом отчете анализируются недавно выпущенные ключи дешифрования программ-вымогателей Avaddon, чтобы пролить свет на типы жертв, на которые нацелены злоумышленники, и потенциальный доход, который они получали в ходе своей деятельности.**

11 июня банда вымогателей Avaddon решила прекратить свою деятельность. В рамках завершения работы банда вымогателей анонимно поделилась ключами дешифрования своих жертв с BleepingComputer.

Используя эти ключи, Emsisoft создала дешифратор, который позволяет жертвам бесплатно восстанавливать свои файлы.

Эти ключи дешифрования были выпущены в виде двух текстовых файлов, в которых каждая жертва содержала числовой идентификатор и два криптографических ключа в кодировке base64, которые могли расшифровать файлы жертвы.

Для многих из этих ключей банда программ-вымогателей также включала какой-то идентификатор, который может быть доменом Windows, именем вошедшего в систему пользователя или каким-либо другим идентификатором.

Хотя некоторые из этих идентификаторов свидетельствуют о серьезных кибератаках против ранее неизвестных корпоративных целей, BleepingComputer не намерен сообщать об этих жертвах.

*Данные проливают свет на цели Аваддона*

После анализа уникальных идентификаторов, связанных с ключами дешифрования Avaddon, компания Advanced Intel, занимающаяся кибербезопасностью, опубликовала анонимные сведения о жертвах, на которые нацелена группа программ-вымогателей.

«Сегодня мы пролили свет на эту затерянную и скрытую преступную империю, используя уникальные наборы данных – полный список жертв Avaddon, когда-либо подвергавшихся нападениям этой группировки за год ее существования», – говорится в отчете Advanced Intel.

Из жертв, на которые нацелился Аваддон, большинство организаций проживали в США, затем в Канаде, а затем и во всем мире. Как отмечается на карте, известных жертв в России или других странах СНГ, что характерно для группировок вымогателей, не было.

Три основных сектора, на которые ориентируется Avaddon, – это розничная торговля (12,5%), производство (12,2%) и (6,3%) и финансы (7,5%). Однако Avaddon нацелился на широкий круг компаний, и хотя злоумышленники нацелены на одни отрасли больше, чем на другие, это, вероятно, все еще были оппортунистические атаки.

Наконец, используя список известных жертв, Advanced Intel сгруппировала их по годовому доходу, показав, что более 50% получили доход ниже 10 миллионов долларов.

В среднем, доходы жертв Аваддона составляют:

13 миллионов долларов США для малого бизнеса

287 миллионов долларов для жертв среднего размера

3,7 миллиарда долларов США для крупного бизнеса

Источник Advanced Intel утверждает, что Avaddon использует правило «5x5» при определении требований о выкупе.

«Наиболее распространенным расчетом, который, согласно нашим конфиденциальным и достоверным источникам информации, используемым Avaddon, было так называемое правило «5x5», когда 5% годового дохода используется для начала переговоров, а годовой доход оценивается в одну пятую общая выручка», – поясняется в отчете.

Другими словами, для жертвы, имеющей общий доход в 7 миллионов долларов США, начальная цена выкупа будет составлять 70 000 долларов США. Обычно Avaddon понижал цену во время переговоров, а конечный выкуп составлял около 50 000 долларов США за успешную операцию».

Используя эту информацию и внутренние данные, основанные на известных жертвах, Advanced Intel считает, что общий доход Avaddon составляет около 87 миллионов долларов.

«Отзывы от высокопоставленных членов подпольного сообщества, которые, как сообщается, работали с Avaddon, а также с другими коллекциями из DarkWeb, хотя мы смогли составить приблизительный шаблон для каждой трехмерной жертвы, заплатившей выкуп», – сказал BleepingComputer Елисей Богуславский из Advanced Intel.

«Эта закономерность коррелирует с нашим опытом устранения инцидентов, связанных с программами-вымогателями».

Непонятно, почему Avaddon прекратил свою деятельность, но считается, что это связано с усилением давления со стороны правительства и правоохранительных органов США.

Хотя программы-вымогатели представляют собой проблему с 2012 года, только в последние два года правоохранительные органы успешно прервали эти операции.

Это нарушение было успешным, поскольку оно нацелено на аффилированных лиц, инфраструктуру и платежи, а не на основных разработчиков программы-вымогателя». ***(Lawrence Abrams. Avaddon ransomware's exit sheds light on victim landscape // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/avaddon-ransomwares-exit-sheds-light-on-victim-landscape/). 15.06.2021).***

***

**«Новая программа-вымогатель PayloadBIN была приписана киберпреступной банде Evil Corp, которая провела ребрендинг, чтобы избежать санкций, введенных Управлением по контролю за иностранными активами Министерства финансов США (OFAC).**

Банда Evil Corp, также известная как Indrik Spider и банда Dridex, начинала как филиал ботнета ZeuS. Со временем они сформировали группу, которая сосредоточилась на распространении банковского трояна и загрузчика под названием Dridex через фишинговые электронные письма.

Когда киберганги начали переходить к высокодоходным атакам программ-вымогателей, Evil Corp запустила операцию вымогателя под названием BitPaymer, которая доставлялась через вредоносное ПО Dridex в скомпрометированные корпоративные сети.

После санкций со стороны правительства США в 2019 году фирмы, занимающиеся переговорами о программах-вымогателях, отказались уплатить выкуп за атаки программ-вымогателей Evil Corp, чтобы избежать штрафов или судебных исков со стороны Министерства финансов.

Evil Corp начала переименовывать свои операции с программами-вымогателями на разные имена, такие как WastedLocker, Hades и Phoenix, чтобы обойти эти санкции.

Злоумышленники использовали Phoenix для атаки на страховую компанию CNA.

*Evil Corp выдаёт себя за хакерскую группу Payload Bin*

После взлома столичного департамента полиции в Вашингтоне, округ Колумбия, и кражи незашифрованных данных банда Бабука заявила, что

отказывается от шифрования с помощью программ-вымогателей и вместо этого сосредоточивается на краже и вымогательстве данных.

В конце мая сайт утечки данных Babuk был обновлен, и банда вымогателей была переименована в новую группу под названием «ящик полезной нагрузки»…

В четверг BleepingComputer обнаружил новый образец вымогателя под названием PayloadBIN [VirusTotal], который, как мы сразу предположили, был связан с ребрендингом Babuk Locker.

После установки программа-вымогатель будет добавлять расширение .PAYLOADBIN к зашифрованным файлам…

Кроме того, записка с требованием выкупа называется «PAYLOADBIN-README.txt» и заявляет, что «сети жертвы ЗАБЛОКИРОВАНЫ с помощью программы-вымогателя PAYLOADBIN».

Обнаружив образец, BleepingComputer решил, что Babuk лжет об их намерениях отказаться от программ-вымогателей и переименовался в новое имя.

Однако после анализа новой программы-вымогателя Фабиан Восар из Emsisoft и Майкл Гиллеспи из ID Ransomware подтвердили, что программа-вымогатель представляет собой ребрендинг предыдущих операций вымогателей Evil Corp.

Обсуждая, почему они выдавали себя за другую киберпреступную группу, Восар почувствовал, что они увидели и воспользовались возможностью, чтобы выдать себя за хакерскую группу, которая не подверглась санкциям.

«Теперь у них был ребрендинг банды, и они просто воспользовались возможностью». – Фабиан Восар.

Поскольку программа-вымогатель теперь приписывается санкционированной группе хакеров, большинство фирм, занимающихся переговорами о программах-вымогателях, скорее всего, не помогут упростить выплаты жертвам, пострадавшим от вымогателя PayloadBIN». ***(Lawrence Abrams. New Evil Corp ransomware mimics PayloadBin gang to evade US sanctions // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-evil-corp-ransomware-mimics-payloadbin-gang-to-evade-us-sanctions/). 06.06.2021).***

***

**«Тайваньский ведущий производитель памяти и устройств хранения данных ADATA заявляет, что атака программы-вымогателя вынудила его отключить системы после того, как в конце мая была поражена его сеть.**

ADATA производит высокопроизводительные модули памяти DRAM, карты флэш-памяти NAND и другую продукцию, включая мобильные аксессуары, игровые продукты, электропоезда и промышленные решения.

В 2018 году компания была признана вторым по величине производителем памяти DRAM и твердотельных накопителей (SSD).

*ADATA подтверждает майскую атаку программ-вымогателей*

Тайваньский производитель памяти отключил все затронутые системы после обнаружения атаки и уведомил все соответствующие международные органы об инциденте, чтобы помочь отследить злоумышленников.

«Компания ADATA подверглась атаке программы-вымогателя 23 мая 2021 года», – сообщила компания BleepingComputer в сегодняшнем электронном письме.

Согласно заявлению производителя памяти, бизнес-операции ADATA больше не прерываются: поврежденные устройства восстанавливаются, а службы прекращают работу.

«Компания успешно приостановила работу затронутых систем, как только была обнаружена атака, и были предприняты все необходимые усилия для восстановления и обновления соответствующих систем ИТ-безопасности», – добавила ADATA.

«К счастью, все движется в нормальное русло, и бизнес-операции не прерываются, поскольку соответствующие меры на случай непредвиденных обстоятельств эффективны.

«Мы полны решимости посвятить себя созданию защищенной системы, как никогда, и да, это будет наша бесконечная практика, пока компания движется вперед к своему будущему росту и достижениям».

*Программа-вымогатель Ragnar Locker заявляет об атаке*

ADATA не предоставила информации о действиях программы-вымогателя, стоящей за инцидентом, или о каких-либо требованиях выкупа. Однако в минувшие выходные об атаке уже заявили банды вымогателей Ragnar Locker.

Ragnar Locker сообщает, что они якобы украли 1,5 ТБ конфиденциальных данных из сети ADATA перед развертыванием полезной нагрузки вымогателя.

Пока что банда вымогателей опубликовала только скриншоты украденных файлов и папок в качестве доказательства своих заявлений, но они угрожают утечкой остальных данных, если производитель памяти не заплатит выкуп.

Согласно снимкам экрана, уже размещенным Ragnar Locker на своем сайте утечки в темной сети, злоумышленники могут собирать и извлекать служебную бизнес-информацию, конфиденциальные файлы, схемы, финансовые данные, исходный код Gitlab и SVN, юридические документы, информацию о сотрудниках, соглашения о неразглашении информации и работу. папки.

Впервые активность программы– вымогателя Ragnar Locker была обнаружена в ходе атак на несколько целей в конце декабря 2019 года.

На скомпрометированных корпоративных конечных точках операторы Ragnar Locker завершают работу программного обеспечения удаленного управления (например, ConnectWise и Kaseya), используемого поставщиками управляемых услуг (MSP) для удаленного управления системами клиентов.

Это позволяет злоумышленникам избежать обнаружения и гарантировать, что администраторы, вошедшие в систему удаленно, не заблокируют процесс развертывания полезной нагрузки.

ФБР предупредило партнеров из частного сектора об увеличении активности программ-вымогателей Ragnar Locker после атаки в апреле 2020 года, которая затронула сеть транснационального энергетического гиганта Energias de Portugal (EDP).

По данным BleepingComputer, требования выкупа Ragnar Locker варьируются от 200000 до примерно 600000 долларов. Однако Рагнар Локер потребовал выкуп в размере 1580 биткойнов (эквивалент более 10 миллионов долларов) в случае EDP».

***(Sergiu Gatlan. Computer memory maker ADATA hit by Ragnar Locker ransomware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/computer-memory-maker-adata-hit-by-ragnar-locker-ransomware/). 08.06.2021).***

***

**«Министерство труда и социальной экономики Испании (MITES) работает над восстановлением услуг после кибератаки в среду.**

MITES – это министерский департамент с годовым бюджетом почти в 39 миллионов евро, которому поручено координировать и контролировать политику занятости, социальной экономики и корпоративной социальной ответственности Испании.

«Министерство труда и социальной экономики подверглось компьютерной атаке», – сообщило сегодня агентство MITES.

«Технические менеджеры Министерства и Национального криптологического центра работают вместе, чтобы определить происхождение и восстановить нормальное состояние как можно скорее».

Несмотря на то, что веб-сайт министерства все еще работает после атаки, и офис связи, и мультимедийный зал не работают.

Испанская Servicio Público de Empleo Estatal (SEPE) – правительственное учреждение, входящее в состав MITES, которое в марте было поражено программой-вымогателем – заявляет, что кибератака не затронула его.

«Компьютерная атака, которой подверглось Министерство труда и социальной экономики, НЕ повлияла на работу Государственной службы занятости населения», – говорится в сообщении SEPE.

«Электронный офис, сайт и набор услуг продолжают работать в обычном режиме».

Государственное агентство по трудоустройству пострадало от программы-вымогателя

Кибератака на системы MITES произошла после атаки программы-вымогателя Ryuk, поразившей сеть SEPE три месяца назад, 9 марта.

Инцидент затронул более 700 офисов агентств по всей Испании после того, как операторы Ryuk зашифровали сетевые системы агентства.

Согласно объявлению, опубликованному на веб-сайте агентства в то время, программа-вымогатель также распространилась за пределы рабочих станций SEPE и достигла ноутбуков удаленных сотрудников агентства.

В результате атаки программы-вымогателя, поразившей сеть SEPE, сотни тысяч встреч, назначенных через агентство, были отложены по всей Испании.

Испанское агентство по трудоустройству – не единственная известная жертва испанского вымогателя. Everis, ведущий испанский провайдер управляемых услуг (MSP), и Cadena SER (Sociedad Española de Radiodifusión), крупнейшая радиостанция Испании, также были атакованы программами-вымогателями в ноябре 2019 года.

Telefonica, одна из крупнейших телекоммуникационных компаний в мире, также пострадала от атаки вымогателя WannaCry во время вспышки, унесшей десятки тысяч жертв по всему миру в 2017 году». ***(Sergiu Gatlan. Spain's Ministry of***

***Labor and Social Economy hit by cyberattack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/spains-ministry-of-labor-and-social-economy-hit-by-cyberattack/). 09.06.2021).***

***

**«Служба здравоохранения Ирландии столкнулась с проблемами в течение нескольких месяцев, поскольку она продолжает восстанавливаться после атаки с использованием программ-вымогателей, предупредил глава Управления здравоохранения (HSE).**

14 мая HSE, отвечающая за здравоохранение и социальные услуги в Ирландии, стала жертвой «серьезной» атаки с использованием программ-вымогателей.

Атака была приписана банде вымогателей Conti. Киберпреступники бесплатно предоставили НИУ ВШЭ инструмент для дешифрования, но пригрозили опубликовать украденную в результате атаки информацию, что потенциально является нарушением конфиденциальности пациентов, если они не получат выкуп в размере 20 миллионов долларов в биткойнах, чего НИУ ВШЭ не обещала. платить.

Но даже с правильным ключом дешифрования восстановление сети было медленной и сложной задачей для HSE. Медицинские услуги по всей Ирландии по-прежнему не работают, поскольку больницы пытаются лечить пациентов, несмотря на ограниченные ИТ-услуги и отсутствие доступа в Интернет, а это означает, что приемы на прием по-прежнему откладываются или отменяются.

«Процесс восстановления и сопутствующая комплексная проверка обязательно займут некоторое время. Хотя мы можем эффективно расшифровать данные, это только один элемент. Вредоносное ПО также должно быть уничтожено», – заявил в Национальном парламенте генеральный директор HSE Пол Рид. Объединенный комитет по здоровью.

«Расшифровка занимает гораздо больше времени, чем исходное шифрование, а устранение включает дополнительные задачи, чтобы гарантировать, что у злоумышленников нет маршрута доступа обратно в наши системы», – добавил он.

Рид рассказал, как HSE расшифровала 75% своих серверов, и теперь персоналу доступны 70% устройств конечных пользователей. Однако ожидается, что сбои в обслуживании пациентов будут продолжаться в течение некоторого времени – несмотря на то, что ИТ-персонал, эксперты по кибербезопасности и силы обороны Ирландии работают семь дней в неделю, чтобы восстановить полностью работоспособное состояние сети.

«Нельзя недооценивать ущерб, нанесенный этой кибератакой. Конечно, есть финансовые затраты, но, к сожалению, также будут и человеческие потери», – сказал Рид. «Я заверяю участников и общественность, что мы делаем все возможное, чтобы восстановить системы. Я также должен предупредить, что, скорее всего, потребуются месяцы, прежде чем системы будут полностью восстановлены».

В связи с продолжающимися сбоями, HSE предупреждает, что отделения неотложной помощи очень загружены из-за сбоев в работе ИТ и ожидаются значительные задержки, в то время как многие рентгеновские приемы отменяются.

Основные и срочные службы, включая вакцинацию от COVID-19, работают, но пациентов предупреждают, что они могут столкнуться с задержками, потому что «системы не работают как обычно» из-за того, что «критические ИТ-системы» по-прежнему не работают после атаки программ– вымогателей.

Рид сообщил Комитету, что после вымогательства будут получены «важные знания о дальнейших мерах защиты, которые могут быть реализованы», и тот факт, что атака вымогателя произошла, означает, что они были «очевидными уязвимостями» в сети.

Он также предупредил, что программы-вымогатели и «высококвалифицированные преступные организации», стоящие за атаками программ-вымогателей, представляют значительный риск для организаций по всему миру.

«Весь мир должен повысить свою квалификацию, – сказал Рид». ***(Danny Palmer. The human cost of ransomware: Disruption to Irish health service will continue for months // ZDNet (https://www.zdnet.com/article/irish-healthcare-ransomware-attack-three-quarters-of-servers-decrypted-but-disruption-to-services-will-continue-for-months/). 24.06.2021).***

***

**«9 июня 2021 года Управление по гражданским правам (OCR) опубликовало кибер-предупреждение, содержащее важные обновления о том, как компании могут защитить свои операции от атак программ-вымогателей.** Рекомендации поступают от Белого дома и Агентства по кибербезопасности и безопасности инфраструктуры. В меморандуме под названием «Что мы призываем вас сделать для защиты от угрозы программ-вымогателей» рассматривается возросшая частота и масштабы инцидентов с программами-вымогателями и содержится призыв к частному сектору присоединиться к усилиям правительства по защите организаций от растущей угрозы таких атак.

Этот меморандум последовал вслед за Указом президента Байдена о повышении кибербезопасности страны и защите сетей федерального правительства, что еще раз указывает на приоритетность кибербезопасности в федеральном правительстве и частных организациях. Наряду с предоставлением важных рекомендаций для частных лиц в меморандуме также освещаются усилия правительства по разработке согласованной и последовательной политики в отношении выплат выкупа, обеспечения быстрого отслеживания и пресечения доходов в виртуальной валюте и работы с международным сообществом для удержания стран, укрывающих субъектов-вымогателей подотчетен.

Предоставление конкретных шагов частные лица могут следовать, памятку подталкивает предприятия сделать следующее, чтобы увеличить кибербезопасность: (1) осуществлять пять лучших практик из президента Распоряжения, в том числе, например,: многофакторной аутентификации и шифрования данных, (2) назад обновлять данные, регулярно тестировать системы и

сохранять резервные копии в автономном режиме, (3) оперативно обновлять и исправлять системы, (4) тестировать планы реагирования на инциденты, (5) оценивать действия группы безопасности организации с помощью стороннего тестировщика для определения готовности к кибербезопасности и (6) сегментируйте сети компании таким образом, чтобы в случае компрометации сети ущерб был уменьшен.

Хотя меморандум предоставляет жизненно важные и своевременные рекомендации по практике кибербезопасности для частных лиц, в целом он не имеет обязательной силы. Однако необязательный характер меморандума не должен создавать ложное ощущение ограниченной ответственности. OCR продемонстрировало, что будет собирать крупные денежные выплаты от регулируемых организаций, которые не могут должным образом защитить свои сети и системы от кибератак. Например, OCR устранила утечку данных с CHSPSC LLC (CHSPSC) после того, как поставщик информационных технологий (ИТ) разрешил хакерам доступ к ИТ-информации поставщика медицинских услуг с использованием скомпрометированных учетных данных администратора. CHSPSC согласился заплатить 2,3 миллиона долларов для урегулирования этого вопроса. Расследование OCR выявило «системное несоблюдение» правил безопасности HIPAA со стороны CHSPSC, несмотря на явное предупреждение ФБР о попытке взлома. «Отрасль здравоохранения – известная цель для хакеров и кибер-воров. Неспособность реализовать меры безопасности, требуемые правилами HIPAA, особенно после того, как ФБР уведомило о потенциальном нарушении, непростительно», – сказал Северино.

Мы продолжим сообщать о любых дополнительных инструкциях, предоставленных OCR, поскольку они стремятся помочь правительству в усилиях по кибербезопасности в государственном и частном секторах. Если у вас есть какие-либо вопросы, связанные с передовыми методами кибербезопасности, потенциальной ответственностью или рекомендациями OCR, не стесняйтесь обращаться к адвокатам по вопросам здравоохранения в Reed Smith». ***(Catherine David. Office of Civil Rights shares critical cybersecurity guidance amid string of ransomware attacks // Reed Smith LLP (https://www.healthindustrywashingtonwatch.com/2021/06/articles/department-of-health-and-human-services/office-of-civil-rights-shares-critical-cybersecurity-guidance-amid-string-of-ransomware-attacks/#page=1). 24.06.2021).***

***

**«Правительство США и Европы будет координировать борьбу с атаками программ-вымогателей, число которых в последние годы резко возросло, заявил во вторник высокопоставленный представитель службы безопасности США.**

«Теперь у нас есть новая рабочая группа по программам-вымогателям, которая занимается проблемой программ-вымогателей, которые так сильно пострадали в США и во многих других странах. Мы понимаем, что уязвимости одной, мы все разделяем эти уязвимости», – сказал министр внутренней

безопасности Алехандро Об этом заявил Майоркас после встречи с министрами юстиции и внутренних дел европейских стран в Лиссабоне.

«Это то, что мы разделяем, это увеличение числа атак программ-вымогателей во время пандемии, и это та область, где мы, несомненно, можем сделать больше вместе», – сказала Илва Йоханссон, комиссар ЕС по внутренним делам.

В мае киберпреступники остановили крупнейшую в США систему трубопроводов бензина, принадлежащую компании Colonial, а также операции мясоперерабатывающей компании JBS в США. В том же месяце в Ирландии в результате атаки программы-вымогателя была повреждена система здравоохранения страны.

Эксперты по безопасности указали на киберпреступные группы, базирующиеся в России, для атак.

В совместном заявлении ЕС и США говорится, что ЕС и США будут работать вместе «посредством правоохранительных действий, повышая осведомленность общественности о том, как защищать сети, а также о риске выплаты виновным преступникам, и поощрять те государства, которые закрывают глаза на это преступление для ареста и экстрадиции или эффективного преследования преступников на их территории».

Майоркас сказал, что ЕС и США хотят бороться с атаками «путем обмена информацией... путем обмена передовым опытом и совместной работы». ***(LAURENS CERULUS, CLOTHILDE GOUJARD. EU, US launch initiative against ransomware // POLITICO (https://www.politico.eu/article/eu-us-launch-ransomware-cooperation-group/). 22.06.2021).***

***

**«…Недавние перебои в энергоснабжении и пищевой цепи выявили, что программы-вымогатели представляют собой серьезную угрозу кибербезопасности, которая существовала в течение последних нескольких лет.** Больницы, компании, предоставляющие финансовые услуги, фирмы, оказывающие профессиональные услуги, оборонные подрядчики и другие производители, энергетические компании, авиакомпании и другие транспортные компании – все они подвергались атакам со стороны злоумышленников, стремящихся вымогать выкуп в обмен на обещание ключей дешифрования. По состоянию на апрель 2021 года наибольшее количество атак с использованием программ-вымогателей подверглось шести отраслям: здравоохранение, коммунальные услуги, страхование / юридические услуги, поставщики программного обеспечения, производители и ISP / MSP. 1

Программы-вымогатели получили более широкое распространение с распространением программ-вымогателей как услуги, позволяющей разработчикам программ-вымогателей эффективно использовать франшизу или предоставлять других в качестве злоумышленников. Атаки программ-вымогателей также стали более пагубными, поскольку злоумышленники обычно извлекают данные перед запуском вредоносного ПО для шифрования и оказывают большее давление на жертв, чтобы они заплатили под угрозой публикации.

С этим изменением подхода изменился и правовой анализ программ-вымогателей. В прошлом жертвы могли утверждать, что шифрование данных в их собственных системах не вызовет применимых требований к уведомлению о нарушениях, которые обычно включают несанкционированное получение или неправомерное использование определенных данных, часто с порогом, при котором не требуется сообщать о происшествии. не представлять разумной вероятности причинения вреда (в некоторых штатах, ограничиваясь риском кражи личных данных или мошенничества) пострадавшим лицам. Однако, учитывая, что кража данных злоумышленниками становится все более распространенным явлением, одни и те же требования к уведомлению о взломе применяются по-разному. Сложнее поддерживать позицию, согласно которой эксфильтрованные данные не были «приобретены» и что их захват злоумышленником (в зависимости от типа данных) не представлял риска причинения вреда. Следовательно,

В недавнем прошлом казалось, что большинство злоумышленников-вымогателей использовали дробовик: найти выход, запустить атаку и оттуда разобраться. Однако сегодня атаки программ-вымогателей часто проводятся в связи со значительной разведкой и сбором информации о жертве. Разведка может включать сбор информации о жертве и ее платежеспособности, в том числе о существовании и ограничениях страхового покрытия, а также о данных, чтобы сосредоточиться на более ценных данных, чтобы оправдать более высокие требования.

Из-за этих повышенных рисков резко выросли объемы спроса и суммы фактических платежей. Согласно ежеквартальному отчету Coveware, компании по реагированию на программы-вымогатели,

Средний спрос на платежи с использованием цифрового вымогательства резко вырос в первом квартале [2021 года] до 220 298 долларов США, что на 43% больше, чем в предыдущем квартале. 2

Фирма по анализу цепочки блоков Chainalysis подтвердила увеличение выплат:

Известные выплаты злоумышленникам-вымогателям выросли на 337% с 2019 по 2020 год, когда они достигли криптовалюты на сумму более 400 миллионов долларов. Злоумышленники не проявляют признаков замедления активности в 2021 году и уже получили от жертв более 81 миллиона долларов в этом году. Важно помнить, что это нижние оценки, и что истинные цифры почти наверняка выше. 3

Эти статистические данные также предшествуют громким суммам, которые, как сообщается, выплачиваются Colonial Pipeline, JBS и другими.

*Что может быть сделано?*

Упражняйтесь в профилактике. Большинство атак программ-вымогателей осуществляется посредством фишинговых атак. Обучение осведомленности приносит свои плоды в этой среде. Технические меры безопасности, такие как многофакторная аутентификация для предотвращения продолжения удаленного доступа после взлома учетных данных и (где это возможно) ограничения удаленного доступа из ненужных мест, обеспечивают очевидную ценность. Злоумышленникам доступны и другие точки входа, поэтому тестирование на

проникновение, закрытие любых открытых портов и проверка настроек брандмауэра также обеспечивают высокую окупаемость инвестиций.

Но приготовьте «фунт лекарства». Знание того, какие данные хранятся в каких системах до атаки, может сэкономить драгоценное время и уменьшить неопределенность. После того, как данные зашифрованы, может быть трудно подготовиться к планам уведомления и выполнить их, если характер данных и личность затронутых лиц не могут быть определены из-за шифрования. Примите все обычно рекомендуемые шаги по обеспечению готовности к инцидентам, например, создайте свою команду; обновление плана реагирования на инциденты и аварийного восстановления с учетом особенностей атаки программ-вымогателей; просмотр вашего страхового полиса; перепроверка настроек журнала и сохранения; и пересмотр безопасности и адекватности ваших резервных копий». ***(Ransomware's Scary – Be Wary and Ready to Parry – JD Supra // Ransomware Daily (https://ransomwaredaily.com/ransomwares-scary-be-wary-and-ready-to-parry-jd-supra/). 23.06.2021).***

***

**«Британский модный бренд French Connection, который рекламируется под аббревиатурой FCUK, подтвердил, что он был взломан группой программ-вымогателей REvil. Спустя всего несколько часов бразильская медицинская диагностическая компания Grupo Fleury объявила о том же несчастье.**

Двойные атаки раскрывают меняющиеся стратегии и мотивы одного из самых опасных злоумышленников в мире.

Многочисленная банда программ-вымогателей, также известная как Sodinokibi, смогла взломать внутренние серверы French Connection и украсть личные данные руководителей компании.

Компания подтвердила нарушение в своем заявлении, но подчеркнула, что у них «нет доказательств» того, что данные клиентов были скомпрометированы во время атаки, добавив, что бизнес «продолжает работать в основном в обычном режиме».

Регистр подтвердил, что среди украденных файлов были сканы паспортов и удостоверений личности топ-менеджеров компании, основателя и генерального директора Стивена Маркса, финансового директора Ли Уильямса и главного операционного директора Нила Уильямса.

«Как только стало известно о взломе, компания немедленно приняла меры, приостановив работу всех затронутых систем и привлекла сторонних экспертов для оказания помощи в разрешении ситуации», – говорится в заявлении French Connection. «В настоящее время компания активно работает над тем, чтобы восстановить свои системы как можно быстрее и безопаснее, и при необходимости использует ручные корректировки, чтобы гарантировать, что компания может продолжать работать».

Тем временем бразильская компания по медицинской диагностике Grupo Fleury была атакована программой-вымогателем REvil во вторник и поздно вечером 23 июня объявила, что работает над возобновлением работы.

REvil требует 5 миллионов долларов за отправку Grupo Fleury дешифратора, сообщает BleepingComputer.

*Что FCUK и Grupo Fleury Attacks говорят о REvil*

Джейми Харт, аналитик по анализу угроз из Digital Shadows, рассматривает две атаки REvil несколько иначе, объясняя, что атака French Connection, вероятно, была одной из возможностей, чтобы доказать, что любая компания может быть взломана в любом месте.

Атака на Grupo Fleury является частью более широкой кампании REvil против бразильских компаний. Харт сказал, что группа вымогателей сообщила телеграмм-каналу Russian-OSINT, что они хотят отомстить Бразилии, но неясно, почему.

«Атаки REvil (также известного как Sodinokibi) на Grupo Fleury продолжают свою кампанию против бразильских организаций, – сказал Харт Threatpost. «REvil известен тем, что улавливает данные, и эти данные могут включать в себя личную информацию (PII) и конфиденциальную медицинскую информацию их пациентов и персонала, что может нанести ущерб организации».

Харт добавил, что если требования REvil в отношении программ-вымогателей не будут выполнены, эти данные, скорее всего, вскоре появятся на сайте утечки.

Такое смещение акцента на внутренние данные сотрудников, а не на информацию о клиентах, является новым, как объяснила Threatpost Рита Гуревич, основатель и генеральный директор SPHERE Technology.

«Несколько лет назад программы-вымогатели были в первую очередь ориентированы на потребителей, но недавно мы стали свидетелями перехода на более прибыльную корпоративную арену», – сказал Гуревич. «Эти атаки стали более изощренными: от известной стратегии фишинга, использующей массовую рассылку электронной почты, произошел переход к целевой стратегии целевого фишинга, которую труднее обнаружить и которая имеет гораздо более высокий уровень успеха».

И хотя правоохранительные органы добились определенных успехов в преследовании таких групп, как Clop, вредоносное ПО– вымогатель Emotet и злоумышленник Colonial Pipeline DarkSide, она добавила, что легкость, с которой начинающий киберпреступник может получить доступ к вымогателям, подпитывает рост атак.

*REvil становится все более наглым.*

Ранее в этом месяце группа украла военную документацию США у подрядчика, занимающегося ядерным оружием, и банда вымогателей также взяла на себя ответственность за сокрушительную атаку на JBS Foods.

Действительно ли программы-вымогатели вызывают усталость?

Этот постоянный шум заголовков о программах-вымогателях способствует тому, что Дирк Шрейдер из New Net Technologies назвал «программами-вымогателями выявляют усталость».

«Похоже, нам нужен хэштег вроде #ransomwarealertfatigue или #raf», – сказал Шрейдер Threatpost. «FCUK был не первым и не последним, кого ударили. К сожалению, компании, обычные пользователи и, возможно, также некоторые

профессионалы в области безопасности не обратят на это внимания или даже не обратят внимания. ИТ-безопасность уже находится в состоянии повышенной готовности, и две другие группы, похоже, приспособились к проблеме, не намереваясь менять свой подход к риску».

Гуревич согласился, заявив, что федеральное правительство и сообщество безопасности работают вместе, чтобы изменить позицию компаний от реагирования к предотвращению.

Тем организациям, которые заинтересованы в усилении защиты от кибербезопасности, следует начать с «первых шагов в цепочке кибер-убийств», – добавил Шрейдер. «Ограничьте разведку инфраструктуры, чтобы можно было использовать меньше информации или ее совсем не использовать для вооружения атаки против нее, запретите доставку вредоносных программ, чтобы уменьшить поверхность атаки для использования, и, наконец, обнаруживайте любую установку, любой файл, сброшенный на устройство, как нежелательное изменение статуса и целостности системы». ***(Becky Bracken. Oh FCUK! Fashion Label, Medical Diagnostics Firm Latest REvil Victims // Threatpost (https://threatpost.com/fcuk-fashion-medical-diagnostics-revil/167245/). 24.06.2021).***

***

**«С тех пор, как два известных русскоязычных форума по киберпреступности запретили темы, связанные с программами-вымогателями [1, 2], преступные операции были вынуждены продвигать свои услуги с помощью альтернативных методов.**

По крайней мере, две банды вымогателей, нуждающиеся в хакерах для проведения атак, использовали свои сайты для рекламы функций своих инструментов шифрования с целью привлечения новых сотрудников.

*Хвастовство, чтобы соблазнить партнеров*

Около недели назад банда вымогателей LockBit анонсировала новую основную версию своего инструмента, заявив о значительном улучшении скорости шифрования.

Чтобы подтвердить свое утверждение, злоумышленник, по-видимому, протестировал версии нескольких программ-вымогателей и опубликовал свои измерения скорости шифрования файлов.

Запустив LockBit 2.0, разработчики программ-вымогателей также объявили о новом сеансе набора партнеров, подчеркнув, что используемое ими шифрование не дает сбоев с момента начала операции в сентябре 2019 года.

«Единственное, что вам нужно сделать, это получить доступ к главному серверу, а LockBit 2.0 сделает все остальное. Запуск осуществляется на всех устройствах доменной сети при наличии прав администратора на контроллере домена», – заявляет банда вымогателей LockBit.

Чтобы привлечь партнеров, LockBit утверждает, что предлагает самые быстрые инструменты для шифрования и кражи файлов (StealBit) «во всем мире».

Этот шаг со стороны LockBit был предпринят после того, как в конце мая актер попытался вернуть разговоры о вымогателях на популярном русскоязычном

форуме, предложив приватный раздел только для «авторитетных пользователей, в которых нет никаких сомнений».

Хотя один из пользователей подумал, что это хорошая идея, они также отметили, что тема вымогателей «теперь более известна, чем террористы ИГИЛ», а это означает, что форум получит нежелательное внимание.

Другая банда, недавно продвигающая на своем веб-сайте операцию «программа-вымогатель как услуга» (RaaS), – это компания Himalaya, которая начала свою деятельность в этом году.

За исключением использования своего сайта для распространения информации, Himalaya ничем не отличается от других программ-вымогателей. Они рекламируют 70% комиссию для аффилированных лиц и «уже настроенную и скомпилированную вредоносную программу FUD [Fully UnDetectable]» для шифрования файлов.

Как видно из объявления ниже, Himalaya устанавливает строгие правила в отношении целей и, очевидно, не позволяет атаковать медицинские, общественные и некоммерческие организации.

В то время как BleepingComputer знает, что только LockBit и Himalaya активно рекламируют свои операции RaaS на своих веб-сайтах в настоящее время, другие банды вымогателей могут применить эту тактику, если она окажется успешной.

Компания по анализу угроз KELA заявляет, что не все группы программ-вымогателей так громко ищут партнеров.

Например, банда REvil предпочитает действовать конфиденциально и полагается на свою сеть филиалов и связей, чтобы найти новых партнеров, когда они им понадобятся, говорит KELA.

В середине мая, сразу после того, как программы-вымогатели были заблокированы на одном форуме, группа REvil объявила, что они будут вести свою деятельность в частном порядке.

Другие видные группы, вероятно, будут молчать, учитывая активную охоту на злоумышленников, которая усилилась после того, как DarkSide зашифровала системы Colonial Pipeline, нарушив распределение топлива в США, особенно на Восточном побережье». ***(Ionut Ilascu. Ransomware gangs now creating websites to recruit affiliates // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ransomware-gangs-now-creating-websites-to-recruit-affiliates/). 28.06.2021).***

***

**«Операция вымогателя REvil теперь использует шифровальщик Linux, который нацеливается и шифрует виртуальные машины Vmware ESXi.**

По мере того, как предприятия переходят на виртуальные машины для упрощения резервного копирования, управления устройствами и эффективного использования ресурсов, банды программ-вымогателей все чаще создают собственные инструменты для массового шифрования хранилищ, используемых виртуальными машинами.

В мае Елисей Богуславский из Advanced Intel поделился сообщением на форуме о работе REvil, в котором они подтвердили, что выпустили версию своего шифратора для Linux, которая также может работать на устройствах NAS.

Сегодня исследователь безопасности MalwareHunterTeam обнаружил версию вымогателя REvil для Linux (также известную как Sodinokibi), которая также нацелена на серверы ESXi.

Виталий Кремез из Advanced Intel, который проанализировал новый вариант REvil Linux, сказал BleepingComputer, что это исполняемый файл ELF64 и включает те же параметры конфигурации, что и более распространенный исполняемый файл Windows.

Кремез заявляет, что это первый известный случай, когда вариант Linux стал общедоступным с момента его выпуска.

При выполнении на сервере злоумышленник может указать путь для шифрования и включить тихий режим...

При выполнении на серверах ESXi он запускает инструмент командной строки esxcli для вывода списка всех работающих виртуальных машин ESXi и их завершения.

Эта команда используется для закрытия файлов диска виртуальной машины (VMDK), хранящихся в папке / vmfs /, чтобы вредоносная программа-вымогатель REvil могла зашифровать файлы без их блокировки ESXi.

Как пояснил технический директор Emsisoft Фабиан Восар, если виртуальная машина не будет правильно закрыта перед шифрованием файла, это может привести к повреждению данных.

Выбирая таким образом виртуальные машины, REvil может зашифровать сразу несколько серверов с помощью одной команды.

Восар сообщил BleepingComputer, что другие операции с программами-вымогателями, такие как Babuk, RansomExx / Defray, Mespinoza, GoGoogle, DarkSide и Hellokitty, также создали шифровальщики Linux для нацеливания на виртуальные машины ESXi.

«Причина, по которой большинство групп программ-вымогателей внедрили версию своих программ-вымогателей для Linux, состоит в том, чтобы нацеливаться именно на ESXi, – сказал Восар.

Хэши файлов, связанные с шифровальщиком REvil Linux, были собраны исследователем безопасности Хайме Бласко и опубликованы на Open Threat Exchange Alienvault». ***(Lawrence Abrams. REvil ransomware's new Linux encryptor targets ESXi virtual machines // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/revil-ransomwares-new-linux-encryptor-targets-esxi-virtual-machines/). 28.06.2021).***

***

**«Банда вымогателей PYSA использовала трояна удаленного доступа (RAT), получившего название ChaChi, для проникновения в системы здравоохранения и образования и кражи данных, которые впоследствии используются в схемах двойного вымогательства.**

ChaChi – это специальная вредоносная программа RAT на основе Golang, разработанная в начале 2020 года и применяемая операторами PYSA для доступа к зараженным системам и управления ими.

Впервые RAT был замечен в реальных условиях как инструмент, в котором отсутствуют возможности обфускации, переадресации портов и туннелирования DNS. Однако его создатели обновили его, включив в него все эти функции, которые наблюдались при анализе образцов, обнаруженных в последующих атаках.

«После первых наблюдений за атаками в первом квартале 2020 года код ChaChi был изменен, чтобы включить обфускацию и постоянство в конце марта или начале апреля», – говорится в отчете BlackBerry Threat Research and Intelligence Team в отчете, заранее предоставленном BleepingComputer.

«Вскоре после этого мы начали видеть варианты ChaChi с добавленными функциями DNS-туннелирования и перенаправления портов / прокси».

Один из самых ранних образцов ChaChi был развернут в сетях местных органов власти Франции в марте 2020 года. Позже банда программ-вымогателей использовала обновленную версию для нацеливания на различные отраслевые вертикали, от здравоохранения до частных компаний.

Модернизированный ChaChi RAT используется для эскалации атак на образовательные организации

Согласно экстренному предупреждению ФБР, выпущенному в марте 2021 года, эти атаки завершились эскалацией активности программы-вымогателя PYSA, нацеленной на учебные заведения Великобритании и 12 штатов США.

«С марта 2020 года ФБР стало известно об атаках программ-вымогателей PYSA на американские и иностранные государственные учреждения, образовательные учреждения, частные компании и сектор здравоохранения со стороны неустановленных кибер-субъектов», – заявило ФБР.

«Сообщения ФБР указывают на недавний рост числа программ-вымогателей PYSA, нацеленных на учебные заведения в 12 штатах США и Соединенном Королевстве. Неопознанные кибер-акторы специально нацелены на высшее образование, школы K-12 и семинарии».

Тот факт, что организации здравоохранения и образования регулярно работают с огромным количеством конфиденциальной личной и медицинской информации, делает их идеальными жертвами банд вымогателей, таких как PYSA, которые также крадут данные перед шифрованием сетей жертв.

Больницы и школы без резервных копий данных, которые также используют устаревшие и редко исправляемые системы, являются еще более легкой мишенью для злоумышленников, поскольку их легче убедить заплатить выкуп за восстановление систем и вернуть свои украденные данные.

Программа-вымогатель PYSA была впервые обнаружена в октябре 2019 года, когда начали появляться сообщения о компаниях, пострадавших от новой программы-вымогателя.

Эта банда программ-вымогателей известна тем, что крадет широкий спектр конфиденциальных данных с серверов своих жертв, включая личную информацию (PII), информацию о налогах на заработную плату и другие типы данных.

Техническую информацию о ChaChi RAT, а также индикаторы взлома и правила YARA можно найти в отчете исследователей угроз BlackBerry». ***(Sergiu Gatlan. PYSA ransomware backdoors education orgs using ChaChi malware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/pysa-ransomware-backdoors-education-orgs-using-chachi-malware/). 23.06.2021).***

***

***Програми-трояни***

---

**«Вредоносное ПО TeaBot (также известное как Anatsa), впервые появившееся в декабре прошлого года и действующее по сей день, пытается обманом заставить жертвы загрузить троянскую программу для кражи конфиденциальных данных, используя для этого поддельные версии популярных приложений.**

Как рассказали исследователи кибербезопасности из Bitdefender, фальшивые Android-версии антивирусных приложений, медиаплеера VLC, проигрывателей аудиокниг и пр. имеют имена и логотипы, немного отличающиеся от настоящих. Кроме того, они не распространяются через официальный магазин Google Play, а загружаются со сторонних веб-сайтов.

К потенциальным жертвам эти вредоносные приложения попадают, в частности, с помощью поддельного блокировщика рекламы (все способы распространения трояна пока не установлены). Фальшивый Ad Blocker ничего не блокирует, а лишь запрашивает разрешения на отображение поверх других приложений, на показ уведомлений и установку программ из других источников, помимо Google Play. После установки эти приложения работают в скрытном режиме, демонстрируя предупреждения, что смартфон будто бы повреждён вредоносным приложением. Это побуждает пользователя нажать на ссылку для загрузки предлагаемого решения, которым и является TeaBot.

TeaBot позволяет киберпреступникам красть банковские реквизиты и другую конфиденциальную информацию посредством кейлоггинга и кражи кодов аутентификации, а также может взять Android-устройство под полный дистанционный контроль.

Большая часть целевой аудитории TeaBot сосредоточена в Западной Европе, а пик заражений приходится на Испанию и Италию, но жертвами часто становятся и пользователи в Великобритании, Франции, Бельгии, Нидерландах и Австрии.

Помочь пользователям не стать жертвой TeaBot может соблюдение общих предосторожностей. «Никогда не устанавливайте приложения не из официального магазина. Кроме того, никогда не нажимайте на ссылки в сообщениях и всегда думайте, что разрешать вашим приложениям для Android», — так формулируют их эксперты в блоге Bitdefender». ***(Банковский троян TeaBot заражает Android-смартфоны через поддельные приложения // Компьютерное Обозрение (https://ko.com.ua/bankovskij_troyan_teabot_zarazhaet_android-smartfony_cherez_poddelnye_prilozheniya_137569). 02.06.2021).***

***

**«Фишинговая кампания представляет новый вариант одной из старейших форм троянских программ удаленного доступа (RAT) с целью кражи имен пользователей, паролей и другой конфиденциальной информации. Он также направлен на кражу криптовалюты у жертвы.**

Агент Tesla впервые появился в 2014 году и до сих пор остается распространенной формой вредоносного ПО. Вредоносные программы ориентированы на кражу конфиденциальной информации с зараженных машин Windows, с помощью кейлоггер, которая посылает то, что жертва печатает нападающий – позволяя им видеть имена пользователей, пароли и многие другие.

Теперь исследователи Fortinet подробно описали новую кампанию Agent Tesla, которая распространяет обновленную версию вредоносного ПО через фишинговые электронные письма.

Вредоносные сообщения выглядят как деловая электронная почта – например, в одном из них пользователю предлагается открыть вложение Microsoft Excel под названием «Требования к заказу и спецификации». Документ содержит макрос, который при запуске запускает процесс, который выполняет и загружает агент Tesla на машину.

Это выполняется на нескольких различных этапах, включая загрузку файлов PowerShell, запуск сценария VBScript и создание задачи расписания. Все это помогает замаскировать установку вредоносного ПО, позволяя злоумышленнику тайно отслеживать активность на компьютере. Эта версия агента Тесла опрашивает оператора каждые 20 минут, отправляя им любой новый обнаруженный ввод.

В дополнение к этому, атака также захватывает любой биткойн-кошелек на устройстве жертвы. Отслеживая активность на компьютере и злоупотребление кодом PowerShell, злоумышленник может отслеживать действительный адрес биткойнов. Если это обнаруживается, код изменяет адрес биткойна и меняет его на адрес, принадлежащий злоумышленнику, что позволяет им украсть переводы криптовалюты.

Несмотря на то, что Agent Tesla существует с 2014 года, он остается популярным среди киберпреступников, оставаясь эффективным и относительно дешевым: покупка лицензии на подпольных форумах может стоить всего 15 долларов.

Помимо низкой стоимости, авторы Agent Tesla предлагают круглосуточную техническую поддержку без выходных, что позволяет ей служить точкой входа для менее изощренных киберпреступников, при этом потенциально нанося ущерб любому человеку или организации, ставшим жертвой вредоносного ПО.

Многие атаки по-прежнему распространяются с помощью фишинговых писем, а это означает, что, если будут приняты правильные меры предосторожности, можно избежать жертв. Исследователи кибербезопасности рекомендуют использовать антивирусное программное обеспечение для обнаружения подозрительной активности, в то время как пользователи должны быть осторожны, когда дело доходит до открытия вложений из неизвестных источников с неожиданными электронными письмами». ***(Danny Palmer. This phishing email is pushing password-stealing malware to Windows PCs // ZDNet***

***(https://www.zdnet.com/article/this-phishing-email-is-pushing-password-stealing-malware-to-windows-pcs/). 07.06.2021).***

***

## *Операції правоохоронних органів та судові справи проти кіберзлочинців*

---

**«Сегодня гражданка Латвии предстала перед федеральным судом в Кливленде, штат Огайо, по множеству обвинений, связанных с ее предполагаемой ролью в транснациональной организации по борьбе с киберпреступностью, ответственной за создание и развертывание компьютерного банковского трояна и набора программ-вымогателей, известных как «Trickbot».**

55-летняя Алла Витте, также известная как Макс, обвиняется по 19 пунктам из 47 обвинений, в которых она обвиняется в участии в преступной организации, известной как «Trickbot Group», которая использовала вредоносное ПО Trickbot. Trickbot Group действовала в России, Беларуси, Украине и Суринаме и в первую очередь предназначалась для компьютеров жертв, принадлежащих компаниям, организациям и частным лицам, в том числе в Северном округе Огайо и в других местах США. Цели включали больницы, школы, коммунальные предприятия и правительства. Витте, который ранее проживал в Парамарибо, Суринам, был арестован 6 февраля в Майами, Флорида.

«Это обвинение демонстрирует широкие возможности целевой группы Министерства юстиции по вымогательству и цифровому вымогательству», – заявила заместитель генерального прокурора Лиза О. Монако. «Trickbot заразил миллионы компьютеров-жертв по всему миру и использовался для сбора банковских учетных данных и доставки программ-вымогателей. Обвиняемый обвиняется в сотрудничестве с другими членами транснациональной преступной организации для разработки и развертывания цифрового набора вредоносных программ, используемых для нацеливания на предприятия и отдельных лиц по всему миру с целью кражи и выкупа. Эти обвинения служат предупреждением для потенциальных киберпреступников о том, что Министерство юстиции через Целевую группу по программам-вымогателям и цифровому вымогательству и вместе с нашими партнерами будет использовать все имеющиеся в нашем распоряжении инструменты, чтобы разрушить экосистему киберпреступников».

«Вредоносное ПО Trickbot было разработано для кражи личной и финансовой информации миллионов людей по всему миру, что привело к значительному финансовому ущербу и нанесению значительного ущерба критически важной инфраструктуре в США и за рубежом», – заявила исполняющая обязанности прокурора США Бриджит М. Бреннан из Северный округ Огайо. «Федеральные правоохранительные органы, наряду с помощью, предоставляемой международными партнерами, продолжают бороться с программами-вымогателями и вредоносными программами и уничтожать их там, где это возможно. Мы едины в

наших усилиях по привлечению транснациональных хакеров к ответственности за их действия».

«Витте и ее соратники обвиняются в заражении десятков миллионов компьютеров по всему миру с целью кражи финансовой информации и, в конечном итоге, выведения миллионов долларов через скомпрометированные компьютерные системы», – сказал ответственный специальный агент Эрик Б. Смит из Кливлендского поля ФБР Офис. «Кибернетические вторжения и заражение вредоносным ПО требуют значительного времени, опыта и усилий по расследованию, но ФБР будет гарантировать, что эти хакеры будут привлечены к ответственности, независимо от того, где они проживают и насколько анонимны они считают себя».

В обвинительном заключении утверждается, что начиная с ноября 2015 года Витте и другие похитили деньги и конфиденциальную информацию у ничего не подозревающих жертв, включая предприятия и их финансовые учреждения в США, Великобритании, Австралии, Бельгии, Канаде, Германии, Индии, Италии, Мексике, Испании., и Россия с помощью вредоносного ПО Trickbot.

Витте и ее сообщники предположительно работали вместе, чтобы заразить компьютеры жертв вредоносной программой Trickbot, предназначенной для сбора учетных данных для входа в онлайн-банкинг и сбора другой личной информации, включая номера кредитных карт, электронные письма, пароли, даты рождения, номера социального страхования и адреса. Витте и другие также предположительно захватили учетные данные для входа и другую украденную личную информацию, чтобы получить доступ к онлайн-банковским счетам, выполнить несанкционированные электронные переводы денежных средств и отмыть деньги через счета получателей в США и за рубежом.

Согласно обвинительному заключению, Витте работал разработчиком вредоносных программ в Trickbot Group и писал код, связанный с контролем, развертыванием и выплатами программ-вымогателей. Программа-вымогатель сообщила жертвам, что их компьютер был зашифрован, и что им нужно будет приобрести специальное программное обеспечение через биткойн-адрес, контролируемый Trickbot Group, чтобы расшифровать свои файлы. Кроме того, Витте якобы предоставил код Trickbot Group, который отслеживал и отслеживал авторизованных пользователей вредоносного ПО, а также разработал инструменты и протоколы для хранения украденных учетных данных.

Витте обвиняется по одному пункту обвинения в заговоре с целью совершения компьютерного мошенничества и кражи личных данных при отягчающих обстоятельствах; одно обвинение в сговоре с целью совершения мошенничества с использованием электронных средств и банковских операций, затрагивающего финансовое учреждение; восемь пунктов обвинения в банковском мошенничестве, затрагивающем финансовое учреждение; восемь пунктов обвинения в краже личных данных при отягчающих обстоятельствах и один пункт в сговоре с целью отмывания денег. Подсудимый предстал перед мировым судьей США Уильямом Х. Бафманом-младшим из окружного суда США в Северном округе Огайо. В случае признания виновным ей грозит максимальное наказание в виде пяти лет тюрьмы за сговор с целью совершения компьютерного

мошенничества и кражи личных данных при отягчающих обстоятельствах; 30 лет тюрьмы за сговор с целью совершения мошенничества с использованием электронных средств и банковских операций; 30 лет лишения свободы по каждому факту мошенничества в банке; обязательное наказание в виде двух лет за каждую кражу личных данных при отягчающих обстоятельствах, который должен отбываться последовательно с любым другим приговором; и 20 лет тюрьмы за сговор с целью отмывания денег. Судья федерального окружного суда вынесет решение по любому приговору после рассмотрения Руководящих принципов вынесения приговоров в США и других установленных законом факторов.

Офис ФБР в Кливленде расследовал дело.

Дело ведут старший юрисконсульт CS Heath отдела компьютерных преступлений и интеллектуальной собственности уголовного отдела и помощники прокуроров США Дэниел Дж. Ридл и Дункан Т. Браун из Северного округа Огайо.

Это дело является частью Целевой группы Министерства юстиции по программам-вымогателям и цифровому вымогательству, которая была создана для борьбы с растущим числом атак с использованием программ-вымогателей и цифрового вымогательства. В рамках Целевой группы Отдел по уголовным делам, работая с прокуратурой США, уделяет приоритетное внимание срыву, расследованию и судебному преследованию в отношении программ-вымогателей и цифрового вымогательства путем отслеживания и прекращения разработки и развертывания вредоносного ПО, выявления виновных киберпреступников и привлечение этих лиц к ответственности за свои преступления. Департамент через Целевую группу также стратегически нацелен на криминальную экосистему программ-вымогателей в целом и сотрудничает с национальными и зарубежными государственными учреждениями, а также с партнерами из частного сектора для борьбы с этой серьезной преступной угрозой». ***(Latvian National Charged for Alleged Role in Transnational Cybercrime Organization // Department of Justice (https://www.justice.gov/opa/pr/latvian-national-charged-alleged-role-transnational-cybercrime-organization). 04.06.2021).***

***

**«Две зарегистрированные в Кенте ИТ-компании были привлечены к ответственности в Высоком суде Англии и Уэльса за попытки обмануть игроков с помощью фейковых всплывающих окон с целью создания противников технической поддержки.**

Суд услышал, что Msinfosys Support Ltd и MS Global Support Ltd, которыми управляет один и тот же директор, генерировали нежелательные всплывающие сообщения об ошибках, которые появлялись на компьютерах людей.

Когда эти люди позвонили, чтобы проверить, что не так, их заставили поверить в неисправность их техники. Некоторые даже заплатили деньги, чтобы исправить фиктивные проблемы.

Суд услышал, как жертв мошенничества заставили поверить в то, что они имеют дело с «известными компаниями-разработчиками программного обеспечения».

Следователи обнаружили, что директор Викрам Сингх не имел реального контроля ни над одной из компаний, и работа была передана на аутсорсинг индийской компании Underpin Services Private Limited.

Как сообщили в Высоком суде, Викрам Сингх признал, что обе компании являются бизнесом Underpin, и разрешил Underpin торговать в Великобритании.

Ни Msinfosys Support, ни MS Global Support не были уполномочены действовать от имени крупных поставщиков программного обеспечения, и 9 марта оба были ликвидированы «в общественных интересах» в Высоком суде.

Хотя дело рассматривалось в марте, Служба по делам о несостоятельности только что опубликовала официальное заявление по этому делу, объяснив, что в правительственных сообщениях была пауза из-за периода пурды перед местными и общенациональными выборами в мае.

В своем заявлении Эдна Охириа, главный следователь Службы по делам о несостоятельности, заявила: «Msinfosys Support Ltd и MS Global Support Ltd намеренно использовали ложные предлоги для обмана потребителей, при этом многие платили компаниям, полагая, что они имеют дело с известными компаниями-разработчиками программного обеспечения. или их уполномоченных представителей.

«На самом деле обе компании контролировались иностранной компанией, а директор признавал, что ему не было известно, что компания сообщала потребителям.

«Суд признал серьезность этого неправомерного поведения, и оба они были удалены из деловой среды, чтобы защитить общественность от дальнейшего вреда».

Служба по делам о несостоятельности начала конфиденциальное расследование в отношении обеих компаний после жалоб клиентов». ***(Tim Richardson. Brit IT firms wound up by court order after fooling folk into paying for 'support' over fake computer errors // The Register (https://www.theregister.com/2021/06/15/high_court_winds_up_it_scam_companies/). 15.06.2021).***

***

**«Гражданин России Олег Кошкин был осужден по обвинению в использовании службы шифрования вредоносных программ, используемой ботнетом Kelihos для сокрытия полезных нагрузок вредоносных программ и уклонения от обнаружения.**

Кошкин содержится под стражей с тех пор, как был арестован в Калифорнии в сентябре 2019 года, и ему грозит максимальное наказание в виде 15 лет тюрьмы после 20 сентября 2021 года, когда должен быть вынесен приговор.

Гражданин Эстонии Павел Цуркан, его соответчик, также признал сегодня в видеоконференции свою вину по обвинению в пособничестве хакерам и подстрекательству к ним с целью заражения компьютеров жертв по всему миру вредоносным программным обеспечением, включая программы-вымогатели.

Ежемесячные платежи в размере 3000 долларов США за службы шифрования вредоносных программ.

Кошкин управлял Crypt4U.com, Crypt4U.net, fud.bz, fud.re и другими веб-сайтами, которые обещали отображать вредоносные программы (например, бот-сети, трояны удаленного доступа, клавиатурные шпионы, кражи учетных данных и майнеры криптовалюты), которые практически никто не мог обнаружить. основные поставщики антивирусных решений.

«В частности, Кошкин работал с Петром Левашовым, оператором ботнета Kelihos, над разработкой системы, которая позволила бы Левашову шифровать вредоносное ПО Kelihos несколько раз в день», – заявили в Министерстве юстиции.

Кошкин предоставил Левашову специализированную службу шифрования большого объема данных, которая позволила Левашову распространять Kelihos через несколько преступных организаций.

«Левашов использовал ботнет Kelihos для рассылки спама, сбора учетных данных, проведения атак типа «отказ в обслуживании» и распространения программ-вымогателей и другого вредоносного ПО».

В период с мая 2014 года по апрель 2017 года специалист по обслуживанию Kelihos платил Кошкину примерно 3000 долларов в месяц за его услуги в связи с возбуждением уголовного дела, возбужденным после ареста Левашова в Испании.

*Ботнет Kelihos, один из крупнейших в свое время*

Ботнет Kelihos, активный как минимум с 2010 года и один из крупнейших, когда он был отключен в 2017 году, использовался его операторами и другими киберпреступниками, которые арендовали его для рассылки миллионов спам-сообщений в час.

Американские власти заявили, что в то время, когда Левашов снимал возможности рассылки спама Ботнет для цен от $ 100 до $ 300, в соответствии с судебными документами,

Ботнет подвергался трём попыткам удаления в течение нескольких лет подряд, в 2011, 2012 и 2013 годах, и был окончательно отключен в апреле 2017 года.

Когда ФБР наконец его ликвидировало, ботнет Kelihos, как было известно, контролировал по меньшей мере 60 000 взломанных компьютеров по всему миру.

«Управляя веб-сайтом, предназначенным для сокрытия вредоносных программ от антивирусных программ, Кошкин предоставил важную услугу, которая позволила другим киберпреступникам заразить тысячи компьютеров по всему миру», – сказал исполняющий обязанности прокурора США Леонард Бойл от округа Коннектикут.

«Ответчик разработал и эксплуатировал службу, которая была важным инструментом для некоторых из самых разрушительных киберпреступников в мире, в том числе для злоумышленников, – добавил исполняющий обязанности помощника генерального прокурора Николас Л. Маккуэйд из уголовного отдела Министерства юстиции». ***(Sergiu Gatlan. US convicts Russian national behind Kelihos botnet crypting service // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/us-convicts-russian-national-behind-kelihos-botnet-crypting-service/). 16.06.2021).***

***

**«Министерство юстиции США (DOJ) объявило сегодня, что многонациональная операция уничтожила Slilpp, крупнейший онлайн-рынок украденных учетных данных.**

Правоохранительные органы США, Германии, Нидерландов и Румынии захватили серверы, на которых размещалась инфраструктура торговой площадки Slilpp и ее доменные имена.

Веб-сайты торговой площадки теперь заменены баннером захвата в чистой сети и отображением ошибки неверного адреса лукового сайта в темной сети.

Во время международной операции ФБР работало в сотрудничестве с прокурорами и следователями из нескольких юрисдикций по всему миру.

Агентства, вовлеченные в срыв Slilpp, включают Bundeskriminalamt Германии, Национальное подразделение по преступлениям в сфере высоких технологий Нидерландов и Управление Румынии по расследованию организованной преступности и терроризма.

«Slilpp – это крупнейшая торговая площадка для взломанных учетных записей, которую когда-либо видели в преступном подполье», – сказал BleepingComputer генеральный директор Advanced Intelligence Виталий Кремез.

«Торговая площадка была ответственна за крупные потоки скомпрометированных данных, которые принесли администраторам миллионы долларов незаконной прибыли».

Slilpp действует с 2012 года и использовался киберпреступниками для продажи и покупки украденных учетных данных для входа в банк, онлайн-платежи, мобильные телефоны, розничные магазины и другие онлайн-аккаунты.

Клиенты, купившие учетные данные у поставщиков Slilpp, впоследствии использовали их в несанкционированных транзакциях (например, телеграфные переводы), причем более десятка человек уже были обвинены или арестованы правоохранительными органами США после расследований, связанных с рынком Slilpp.

«Согласно письменным показаниям, часть потерпевших поставщиков аккаунтов на данный момент подсчитала убытки; на основании ограниченных существующих отчетов о жертвах украденные учетные данные, проданные через Slilpp, были использованы для причинения убытков в США на сумму более 200 миллионов долларов. Влияние Slilpp пока не известно», – сказали в Министерстве юстиции.

Прямо перед закрытием торговой площадки и захватом ее сайтов поставщики Slilpp продали более 80 миллионов украденных учетных данных, принадлежащих пользователям более чем 1400 компаний, многие из которых являются известными.

«Торговая площадка Slilpp якобы нанесла жертвам по всему миру убытки на сотни миллионов долларов, в том числе позволив покупателям украсть личности американских жертв», – добавил исполняющий обязанности помощника генерального прокурора Николас Л. Маккуэйд из уголовного отдела Министерства юстиции.

В то время как Slilpp был закрыт, другие крупные торговые площадки остаются в сети, чтобы предоставить киберпреступникам украденные учетные данные.

Например, передовые исследователи безопасности Intel тайно собирали учетные данные для 1,3 миллиона скомпрометированных серверов удаленного рабочего стола Windows в течение почти трех лет после получения доступа к базе данных UAS.

UAS (сокращение от Ultimate Anonymity Services) – крупнейший хакерский рынок украденных учетных данных RDP: в апреле было выставлено на продажу 23 706 учетных записей». ***(Sergiu Gatlan. Slilpp, the largest stolen logins market, seized by law enforcement // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/slilpp-the-largest-stolen-logins-market-seized-by-law-enforcement/). 10.06.2021).***

***

**«Служба інформації та безпеки Молдови (СІБ) спільно з прокуратурою Кишинева запобігли злому урядових інформаційних мереж…**

Зокрема, 29-річний чоловік намагався незаконно авторизуватися в державних інформаційних системах, що належать Службі інформаційних технологій та кібербезпеки.

Під час обшуку у підозрюваного знайшли сервери, вторинне обладнання для забезпечення їх безперебійної роботи і три стаціонарних комп'ютери для управління злочинною діяльністю.

Підозрюваному, який перебував під підпискою про невиїзд на час слідства, вдалося покинути Молдову через КПП у Придністров'ї, непідконтрольний владі країни. Чоловіка оголосили в міжнародний розшук.

За цей злочин йому загрожує від 3 до 7 років в'язниці. СІБ і прокуратура продовжують розслідування…». ***(Молдова попередила кібератаку проти урядових систем // Європейська правда (https://www.eurointegration.com.ua/news/2021/06/17/7124559/). 17.06.2021).***

***

**«Суд у США виніс вирок 33-річному громадянину України Андрію Колпакову через його участь у кіберзлочинному угрупуванні FIN7, яке викрало дані десятків мільйонів кредитних і дебетових карток, що завдало збитків на понад $1 млрд.**

Колпакова засудили до 7 років в'язниці та зобов'язали відшкодувати збитки у розмірі $2,5 млн, повідомляє Міністерство юстиції США.

Ще рік тому українець визнав себе винним за одним із пунктів звинувачення у змові з метою шахрайства з використанням електронних засобів і в змові з метою злому комп'ютера.

Хакера заарештували в Іспанії 28 червня 2018 року, а 1 червня 2019-го на вимогу американських правоохоронних органів екстрадували до США.

Починаючи з 2015 року, члени FIN7 здійснили кібератаки на сотні американських компаній, зламали тисячі комп'ютерних систем і викрали мільйони номерів кредитних та дебетових карток клієнтів, які потім продавали з метою отримання прибутку.

Колпаков брав участь у FIN7 щонайменше з квітня 2016-го. Він також керував іншими хакерами». ***(Валентина Летяк. Українського хакера засудили у США до 7 років в'язниці // ФАКТИ. ICTV (https://fakty.com.ua/ua/svit/20210625-ukrayinskogo-hakera-zasudyly-u-ssha-do-7-rokiv-v-yaznytsi/). 25.06.2021).***

***

## Технічні аспекти кібербезпеки

**«Ангела Меркель во вторник представила компьютер, который использует субатомные частицы для выполнения миллионов вычислений за микросекунды, что сделало Германию претендентом на участие в глобальной гонке за разработку технологии следующего поколения, называемой квантовыми вычислениями.**

«Что касается исследований квантовых технологий, Германия – одна из лучших в мире, и мы намерены оставаться в числе лучших в мире», – сказала канцлер Германии, которая сама является квантовым химиком, во время презентации устройства. «Мы находимся в разгаре очень жесткой конкуренции, и Германия намерена сказать важное слово».

Европа, Соединенные Штаты и Китай вовлечены в конкуренцию за то, кто сможет построить и использовать самые мощные компьютеры. Квантовая технология, которая все еще находится в зачаточном состоянии, обещает выполнять ранее невозможные вычисления с рекордной скоростью. Германия надеется, что квантовые вычисления будут стимулировать инновации во всех отраслях – от транспорта и окружающей среды до здравоохранения.

В то время как традиционные компьютеры обрабатывают «биты» информации, имеющие значение 1 или 0, известные как двоичный код, квантовые компьютеры могут обрабатывать биты, которые могут иметь значение 1 и 0 одновременно, отражая поведение субатомных частиц. Эти квантовые биты, также известные как кубиты, могут выполнять вычисления намного быстрее.

Политики надеются, что технология принесет экономическую выгоду в применении к экономике. Например, беспилотные автомобили могут научиться водить машину безопаснее и быстрее. Технология также обещает взломать сложное шифрование.

Выгоды от квантовых исследований получают страны, которые могут размещать и использовать устройства. Немецкий компьютер, расположенный недалеко от Штутгарта, создается американской технологической компанией IBM и будет управляться Fraunhofer-Gesellschaft, ведущей европейской организацией по прикладным исследованиям. Исследователи и компании смогут разрабатывать и тестировать свои квантовые алгоритмы и собирать знания с помощью компьютера.

Интерес Меркель к технологиям подчеркивает ставки для Германии и других европейских стран, которые пытаются создать местный технологический сектор и отучить себя от иностранных поставщиков. Хотя участие IBM в программе свидетельствует о том, что даже Германии еще нет.

Вместе с несколькими ведущими европейскими квантовыми компаниями IBM предоставляет как компьютер, так и облако, к которому он подключен.

В прошлом году Берлин объявил об инвестициях в квантовые технологии на сумму 2 миллиарда евро в течение пяти лет, а также может получить доступ к фонду Европейской комиссии в размере 1 миллиарда евро для квантовых технологий. Тем не менее Меркель признала, что Европа отстает и ей нужно наверстать упущенное.

«Квантовые вычисления могут сыграть… ключевую роль в наших усилиях по обретению технологического и цифрового суверенитета», – сказал канцлер. «Конечно, не только мы понимаем, что это так. Соединенные Штаты и Китай полностью инвестировали огромные суммы денег».

В настоящее время США и Китай обладают наибольшим количеством патентов на квантовые компьютеры и технологии.

Китайское правительство по сообщениям тратит не менее $ 2,5 млрд в год на квантовом исследовании. В 2018 году Вашингтон выделил 1,2 миллиарда долларов на квантовые исследования в рамках Закона о Национальной квантовой инициативе. Федеральное правительство дополнило финансирование другими инициативами, включая 237 миллионов долларов в бюджете на 2021 год.

Обе страны также могут рассчитывать на своих технологических гигантов, включая Alibaba, IBM и Microsoft.

В условиях напряженных дискуссий в Европе о том, кто контролирует промышленные данные, исследовательский институт Fraunhofer-Gesellschaft будет хранить и обрабатывать данные, производимые компьютерными центрами обработки данных IBM в Германии.

«Заказы будут отправляться на квантовый компьютер, и их можно будет обрабатывать в традиционных компьютерах для обеспечения конфиденциальности данных и суверенитета. Квантовый компьютер будет работать в соответствии с законодательством Германии», – сказал Реймунд Нойгебауэр, президент Fraunhofer-Gesellschaft при запуске.

Он сказал, что институт уже заключил партнерские отношения с компаниями и университетами, которые будут использовать компьютер, но не назвал их имена.

Министр исследований Германии Аня Карличек заявила: «Создание этой экосистемы – очень важный вопрос для безопасности и суверенитета».

«Мы также хотим разработать оборудование для квантовых вычислений здесь, в Германии, и я хотел бы подчеркнуть, что суверенитет не означает, что мы должны изолироваться». ***(CLOTHILDE GOUJARD. Germany unveils powerful quantum computer to keep Europe in global tech race // Politico (https://www.politico.eu/article/germany-unveils-europes-first-quantum-computer/). 15.06.2021).***

***

**«Агентство национальной безопасности (NSA) опубликовало меры по снижению рисков и передовые методы, которым должны следовать системные администраторы при обеспечении безопасности систем обработки вызовов Unified Communications (UC) и передачи голоса и видео по IP (VVoIP).**

UC и VVoIP – это системы обработки вызовов, используемые в корпоративных средах для различных целей, от видеоконференцсвязи до обмена мгновенными сообщениями и совместной работы над проектами.

Поскольку эти системы связи тесно интегрированы с другим ИТ-оборудованием в корпоративных сетях, они также непреднамеренно увеличивают поверхность атаки, создавая новые уязвимости и возможность скрытого доступа к коммуникациям организации.

Неправильно защищенные устройства UC / VVoIP подвержены тем же рискам безопасности и становятся мишенью злоумышленников через шпионское ПО, вирусы, уязвимости программного обеспечения и другие вредоносные средства, если они не защищены и не настроены надлежащим образом.

«Злоумышленники могут проникать в IP-сети, чтобы подслушивать разговоры, выдавать себя за пользователей, совершать мошенничество с платой за проезд и совершать атаки отказа в обслуживании», – пояснили в разведывательном агентстве США.

«Компрометация может привести к тайному сбору аудио и / или видео высокого разрешения в помещении и доставке злоумышленнику, использующему IP-инфраструктуру в качестве транспортного механизма».

Администраторам рекомендуется принять следующие ключевые меры, чтобы минимизировать риск взлома корпоративной сети своей организации путем использования систем UC / VVoIP:

Сегментируйте корпоративную сеть с помощью виртуальных локальных сетей (VLAN) для отделения голосового и видеотрафика от трафика данных.

Используйте списки управления доступом и правила маршрутизации, чтобы ограничить доступ к устройствам через VLAN.

Реализация защиты уровня 2, протокола разрешения адресов (ARP) и защиты от спуфинга IP.

Защитите шлюзы PSTN и периметры Интернета, аутентифицируя все соединения UC / VVoIP

Всегда обновляйте программное обеспечение, чтобы уменьшить уязвимости программного обеспечения UC / VVoIP

Аутентифицировать и шифровать сигнальный и медиа-трафик, чтобы предотвратить выдачу себя за другое лицо и подслушивание злоумышленниками.

Развертывание пограничных контроллеров сеансов (SBC) для мониторинга трафика UC / VVoIP и аудита записей данных вызовов (CDR) с использованием решений для обнаружения мошенничества для предотвращения мошенничества.

Поддерживайте резервные копии конфигураций и установок программного обеспечения для обеспечения доступности

Управляйте атаками типа «отказ в обслуживании» с помощью ограничения скорости и ограничивайте количество входящих вызовов, чтобы предотвратить перегрузку сервера UC / VVoIP.

Используйте идентификационные карты, биометрические данные или другие электронные средства для управления физическим доступом к защищенным областям с помощью сети и инфраструктуры UC / VVoIP.

Проверяйте функции и конфигурации новых (и потенциально несанкционированных) устройств на испытательном стенде, прежде чем добавлять их в сеть.

«Использование преимуществ системы UC / VVoIP, таких как экономия затрат на операции или расширенная обработка вызовов, чревато дополнительным риском», – заключило Агентство национальной безопасности США.

«Система UC / VVoIP представляет новые потенциальные уязвимости безопасности. Поймите типы уязвимостей и способы их устранения, чтобы лучше защитить ваше развертывание UC / VVoIP».

Более обширные передовые методы обеспечения безопасности и меры по снижению рисков, касающиеся подготовки сетей, установления периметров сети, использования контроллеров сеансов предприятия и добавления конечных точек при развертывании систем UC / VVoIP, доступны в Информационном бюллетене по кибербезопасности, выпущенном сегодня АНБ.

В январе NSA также поделилось инструкциями по обнаружению и замене устаревших версий протокола Transport Layer Security (TLS) на современные и безопасные варианты.

Агентство также предупредило компании о необходимости использовать автономные преобразователи DNS-over-HTTPS (DoH), чтобы блокировать попытки перехвата и манипуляции DNS-трафиком злоумышленников». ***(Sergiu Gatlan. NSA shares guidance on securing voice, video communications // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/nsa-shares-guidance-on-securing-voice-video-communications/). 17.06.2021).***

***

## *Виявлені вразливості технічних засобів та програмного забезпечення*

---

**«Эксперты Positive Technologies выявили две уязвимости в прошивке промышленного контроллера WAGO 750-8207. Одна из уязвимостей имеет критический уровень опасности.** Контроллеры серии 750 применяются для автоматизации зданий, при работе с возобновляемыми источниками энергии, на трансформаторных станциях и других объектах энергораспределения, в нефтехимической промышленности, в водопроводах и других коммунальных системах, в судостроительной отрасли, на морских и прибрежных сооружениях, в машиностроении и других сферах. Производитель выпустил обновление безопасности и рекомендации по снижению риска.

Уязвимость CVE-2021-21001 присутствует в компоненте CODESYS 2.3 Runtime, который является частью прошивки контроллеров WAGO. Для эксплуатации уязвимости требуются авторизация и сетевой доступ к контроллеру.

Специалисты WAGO оценили опасность этой уязвимости в 9,1 балла по шкале CVSS 3.0. Ее эксплуатация может привести к получению доступа к файловой системе контроллера с правами на чтение и модификацию. Изменения

файловой системы ПЛК могут повлечь за собой нарушение технологических процессов и различные аварийные ситуации.

Вторая уязвимость, CVE-2021-21000 с оценкой 5,3 балла, обнаружена в сервисе iocheckd, разработанном компанией WAGO, который предназначен для проверки входов и выходов ПЛК, а также отображения конфигурации ПЛК. Для эксплуатации ошибки не требуется авторизация, достаточно иметь сетевой доступ к контроллеру. Ее эксплуатация может привести к внезапному прекращению работы контроллера, что также представляет опасность для непрерывности технологических процессов.

По данным Positive Technologies, в 2020 г. число атак на промышленные компании выросло на 91%». ***(Обнаружена уязвимость в промышленном контроллере WAGO // Компьютерное Обозрение (https://ko.com.ua/obnaruzhena_uyazvimost_v_promyshlennom_kontrollere_wago_137634). 08.06.2021).***

***

**«Хорошая новость – семилетняя ошибка безопасности в Linux Systemd «polkit», используемый во многих дистрибутивах Linux, была исправлена. Плохая новость в том, что это вообще когда-либо было.** Polkit, который systemd использует вместо sudo, позволяет неавторизованным пользователям запускать привилегированные процессы, которые в противном случае они не смогли бы запустить. Оказалось, что вы также можете использовать polkit для получения root-доступа к системе.

*Вы можете сказать «Ой!»?*

Возможность получать привилегии root – это высшее зло в системах Unix и Linux. Кевин Бэкхаус, член лаборатории безопасности GitHub, обнаружил дыру в безопасности полкита во время выполнения своих обязанностей. Он рассказал об этом разработчикам polkit и команде безопасности Red Hat. Затем, когда 3 июня 2021 года было выпущено исправление, оно было публично раскрыто как CVE-2021-3560.

Backhouse обнаружил, что неавторизованный локальный пользователь может легко получить корневую оболочку в системе с помощью нескольких стандартных инструментов оболочки, таких как bash, kill и dbus-send. Как ни странно, хотя ошибка довольно старая, она только недавно появилась в самых популярных дистрибутивах Linux. Например, если вы используете Red Hat Enterprise Linux (RHEL) 7; Debian 10; или Ubuntu 18.04; вы неуязвимы для этой дыры в безопасности. Но если вы используете более новую версию RHEL 8, тестирование Debian; или Ubuntu 20.04, вы можете подвергнуться атаке с его помощью.

Почему? Потому что этот ошибочный код не использовался в большинстве дистрибутивов Linux. Однако недавно уязвимый код был перенесен в готовые версии polkit. Старая дыра в безопасности получила новую жизнь.

Это не единственная причина, по которой этот баг так долго прятался у всех на виду. Бэкхаус объяснил, что дыра в безопасности возникает не каждый раз, когда вы запускаете программы, которые могут ее вызвать. Почему? Оказывается, что polkit запрашивает у dbus-daemon UID [User ID] запрашивающего процесса

несколько раз, с разными путями кода. Большинство этих кодовых путей правильно обрабатывают ошибку, но один из них – нет. Если вы завершите команду dbus-send раньше, она будет обработана одним из правильных путей кода, и запрос будет отклонен. Чтобы активировать уязвимый кодовый путь, вы должны отключиться в нужный момент. А поскольку задействовано несколько процессов, время наступления этого «правильного момента» варьируется от одного запуска к другому. Вот почему для успеха эксплойта обычно требуется несколько попыток. Я предполагаю, что это также причина, по которой ошибка не была

*Это подлая мелочь.*

Но когда Бэкхаус сказал, что это не всегда можно использовать, это не повод не беспокоиться об этом. Вы можете легко написать сценарий, который обязательно активирует его через несколько минут попытки. Red Hat предупреждает: «Самая большая угроза от этой уязвимости – для конфиденциальности и целостности данных, а также для доступности системы».

Поэтому, как указывает Backhouse, поскольку его «очень просто и быстро использовать... важно, чтобы вы как можно скорее обновили свои установки Linux».

Итак, вы знаете, что теперь делать? Приступите к работе над исправлением: обновите polkit до версии 0.119 или более поздней». ***(Steven J. Vaughan-Nichols. Nasty Linux systemd root level security bug revealed and patched // ZDNet (https://www.zdnet.com/article/nasty-linux-systemd-root-level-security-bug-revealed-and-patched/). 16.06.2021).***

***

**«Исследователи говорят, что уязвимости нулевого дня, исправленные в ходе недавнего раунда патчей Microsoft во вторник, использовались в целевых атаках на предприятия.**

По словам Касперского, в течение 14 и 15 апреля 2021 года была отслежена волна «узконаправленных атак» на несколько организаций, которые использовали цепочку эксплойтов нулевого дня в браузере Google Chrome и Microsoft Windows.

Злоумышленники получили название PuzzleMaker. Первым эксплойтом в цепочке, хотя и не подтвержденным, по-видимому, является CVE-2021-21224, уязвимость типа V8 в браузере Google Chrome до 90.0.4430.85.

20 апреля Google выпустил патч для серьезной уязвимости, который в случае использования позволял удаленным злоумышленникам выполнять произвольный код внутри песочницы через созданную HTML-страницу.

Песочницы по своему замыслу предназначены для сред разработки, тестирования и защиты и поэтому отделяют действия от основной системы. Для того, чтобы цепочка эксплойтов сработала, следующим шагом будет выход из песочницы.

По словам исследователей, этот выход был обнаружен в двух уязвимостях Windows 10, обе из которых представляют собой ошибки нулевого дня, исправленные в последнем обновлении Microsoft Patch Tuesday.

Первая, CVE-2021-31955, представляет собой уязвимость ядра Windows для раскрытия информации в файле ntoskrnl.exe, который используется для раскрытия

адресов ядра структуры Eprocess для выполняемых процессов. Вторая, CVE-2021-31956, представляет собой уязвимость, связанную с переполнением буфера кучи в драйвере Windows NTFS, которую можно использовать для повышения привилегий.

По словам Касперского, объединенные в цепочку уязвимости позволили злоумышленнику выйти из песочницы и выполнить вредоносный код на целевой машине.

Затем развертывается вредоносное ПО, которое включает модули stager, dropper, service и remote shell. Первый модуль сначала проверит, что эксплуатация была успешной, и, если да, захватит модуль-дроппер с командно-управляющего (C2) сервера для выполнения.

Затем два исполняемых файла попадают на целевой компьютер, который маскируется под легитимные файлы Windows. Первый зарегистрирован как служба и используется для запуска второго исполняемого файла, который содержит возможности удаленной оболочки.

Эта полезная нагрузка может загружать и извлекать файлы, а также создавать системные процессы. Вредоносная программа также способна на время «усыпить» себя или самоуничтожиться.

Рекомендуется, чтобы организации регулярно составляли графики исправлений и применяли соответствующие исправления – тем более, если ошибки активно используются. Как мы видели в мартовском инциденте с Microsoft Exchange Server, злоумышленники сразу же приступят к решению проблем безопасности, как только они станут общедоступными». ***(Charlie Osborne. PuzzleMaker attacks exploit Windows zero-day, Chrome vulnerabilities // ZDNet (https://www.zdnet.com/article/puzzlemaker-attacks-exploit-windows-chrome-zero-day-vulnerabilities/). 09.06.2021).***

***

**«Управление гражданских прав в действии (OCR) Министерства здравоохранения и социальных служб США выпустило предупреждение о том, что киберпреступники пытаются использовать критическую уязвимость в программном обеспечении VMware.** Это предупреждение исходит от Агентства по кибербезопасности и безопасности инфраструктуры (CISA) и конкретно касается VMware vCenter Server и VMware Cloud Foundation, которые являются частью базовой инфраструктуры, используемой в управлении сетью. Чтобы избежать киберугроз, CISA призывает организации, использующие эти системы, немедленно внедрить необходимые исправления или, если организации не могут сразу применить обновление, применить обходные пути. Тем временем поставщикам медицинских услуг, использующим VMware, особенно рекомендуется немедленно внедрить исправления, чтобы обеспечить защиту защищенной медицинской информации от кибератак, в том числе от программ-вымогателей.

…Отрасль здравоохранения, которая содержит множество ценных данных, таких как номера социального страхования и учетные данные медицинского страхования, является одной из основных целей атак программ-вымогателей.

Фактически, количество нарушений данных в сфере здравоохранения, зафиксированных в 2020 году, увеличилось на 25%., что делает его третьим худшим годом с точки зрения количества взломанных медицинских записей. Самой крупной утечкой данных в сфере здравоохранения в 2020 году стала атака с использованием программ-вымогателей на поставщика облачных услуг Blackbaud Inc., где, как известно, было скомпрометировано более 10 миллионов записей.

Ранее, стремясь усилить то, как отрасль здравоохранения должна бороться с атаками программ-вымогателей, Министерство здравоохранения и социальных служб США (HHS) выпустило информационный бюллетень, направляя медицинские учреждения к Закону о переносимости и подотчетности медицинского страхования (HIPAA), в котором содержатся рекомендации. а также рекомендуемые меры соответствия, чтобы помочь организациям и деловым партнерам, на которые распространяется действие HIPAA, предотвратить программы-вымогатели. А именно, правило безопасности HIPAA требует применения мер безопасности для предотвращения внедрения программ-вымогателей. Защищенные объекты могут снизить риск успешных атак программ-вымогателей:

Проведение анализа рисков для выявления угроз и уязвимостей для электронной защищенной медицинской информации (ePHI) и внедрение мер безопасности для смягчения или устранения этих выявленных рисков;

Внедрение процедур для защиты и обнаружения вредоносного программного обеспечения;

Обучение пользователей защите от вредоносных программ, чтобы они могли обнаруживать вредоносные программы и знать, как сообщать о таких обнаружениях;

Ограничение доступа к ePHI только для тех лиц или программ, которым требуется доступ;

Ведение общего плана действий в чрезвычайных ситуациях, который включает восстановление после бедствий, планирование действий в чрезвычайных ситуациях и периодическое тестирование планов действий в чрезвычайных ситуациях для обеспечения готовности организации;

Понимание программ-вымогателей и определение конкретного вида задействованного вредоносного ПО; а также

*Реализация реагирования на инциденты безопасности.*

После «инцидента безопасности» субъекты, на которые распространяется действие HIPAA, должны инициировать разумные и соответствующие процедуры, процессы реагирования и отчетности. Дополнительное руководство по инцидентам безопасности доступно в Paul Cichonski и др., Руководство по обработке инцидентов компьютерной безопасности: Рекомендации Национального института стандартов и технологий, NIST SP 800-61 Rev.2 (август 2012 г.).

12 мая 2021 г., когда атаки кибербезопасности все еще распространены и растут, президент Байден издал Указ о повышении кибербезопасности страны, который направлен на: (1) устранение барьеров для обмена информацией об угрозах между правительством и частным сектором; (2) модернизировать и внедрить более строгие стандарты кибербезопасности в федеральном

правительстве; (3) повысить безопасность цепочки поставок программного обеспечения; (4) создать комиссию по обзору безопасности кибербезопасности; (5) создать стандартную схему реагирования на киберинциденты; (6) улучшить обнаружение инцидентов кибербезопасности в сетях федерального правительства; и (7) улучшить возможности расследований и исправлений.

В ответ на указ президента Байдена 2 июня 2021 года Энн Нойбергер, заместитель помощника президента и заместитель советника по национальной безопасности по кибербезопасности и новым технологиям, опубликовала меморандум под названием «Что мы призываем вас сделать для защиты от угрозы? Программа-вымогатель». В служебной записке Нойбергера приводятся следующие рекомендации правительства США по снижению риска атак программ-вымогателей:

Внедрение лучших практик от президента Распоряжения;

Резервное копирование данных, системных образов и конфигураций, регулярное их тестирование и сохранение резервных копий в автономном режиме;

Оперативно обновляйте и патчите системы;

Протестируйте свой план реагирования на инциденты;

Проверьте работу вашей службы безопасности; а также

Сегментируйте свои сети.

Медицинские организации должны оценить свое соответствие правилу безопасности HIPAA и реализовать вышеупомянутые меры предотвращения и реагирования для снижения риска и последствий атак программ-вымогателей. В качестве передовой практики крайне важно, чтобы поставщики, использующие системы VMware, своевременно внедряли необходимые исправления, чтобы не дать киберпреступникам воспользоваться уязвимостью в незащищенной системе. Неустановленная система может привести к несанкционированному доступу к конфиденциальной информации о пациенте. Неспособность предотвратить и устранить эти атаки, фактически приводящие к нарушениям HIPAA, могут привести к серьезным штрафам». ***(Elody Tignor. Cybersecurity and HIPAA: Government Issues New Warning and Guidance in Wake of Increased Threats // HOLLAND & HART LLP (https://www.hollandhart.com/showpublication.aspx?Show=39524). 14.06.2021).***

***

**«Ученые из трех немецких университетов обнаружили уязвимость в протоколе безопасности транспортного уровня (TLS), которая при определенных обстоятельствах позволяет кражу файлов cookie сеанса и позволяет атаковать межсайтовые сценарии.**

Дублированный ALPACA, что является аббревиатурой «Application Protocol Layer Путаница – Анализ и смягчающие Трещины в TLS – аутентификации» выводы исследователя описаны в научной статье [PDF], который планируется представить в августе на Black Hat USA 2021 и USENIX безопасности Симпозиум 2021.

Исследователи – Маркус Бринкманн, Роберт Мергет, Йорг Швенк, Йенс Мюллер из Рурского университета в Бохуме, Кристиан Дрезен, Дамиан Поддебняк

и Себастьян Шинцель из Мюнстерского университета прикладных наук, Юрай Соморовский из Падерборнского университета – обнаружили, что TLS не зависит от Уровень приложений в стандартной сетевой модели уязвим для путаницы с сертификатами, если были развернуты подстановочные или многодоменные сертификаты.

Поскольку TLS не связывает TCP-соединения с желаемым протоколом прикладного уровня (например, HTTP, SMTP, IMAP, POP3 и FTP), существует возможность атаки «злоумышленник посередине» (MitM) для перенаправления трафика TLS на другой конечная точка на другом IP-адресе или порту.

«Мы показываем, что в реалистичных сценариях злоумышленник может извлечь файлы cookie сеанса и другие личные данные пользователя или выполнить произвольный JavaScript в контексте уязвимого веб-сервера, таким образом минуя TLS и безопасность веб-приложений», – поясняет документ boffins.

Первая такая атака, описанная два десятилетия назад Йохеном Топфом [PDF], подробно описывает, как браузеры могут быть обмануты для отправки произвольных данных на любой TCP-порт с помощью HTML-форм. Атака ALPACA делает этот метод универсальным для нескольких протоколов.

В обстоятельствах, когда возможна атака MitM (например, локальная сеть или скомпрометированная сетевая система), контролируемый злоумышленником веб-сайт может инициировать HTTPS-запрос из разных источников с вредоносной полезной нагрузкой FTP. Перенаправляя запрос на FTP-сервер с сертификатом, совместимым с веб-сервером, злоумышленник может установить определенный файл cookie через FTP, загрузить вредоносный файл JavaScript через FTP или отразить вредоносный JavaScript в запросе.

*Да, это работает*

Исследователи продемонстрировали, что их метод работает, зарегистрировав учетную запись у провайдера электронной почты Mailfence. Чтобы провести атаку «злоумышленник в браузере» (MitB), они «разместили данные HTML-формы https://mailfence.com:995для входа в [свою] учетную запись и получения содержимого электронного письма в формате HTML (атака загрузки), что привело к выполнению JavaScript в контексте https://mailfence.comдля браузеров, которые игнорируют номер порта в SOP [политика одинакового происхождения], таких как Internet Explorer. Проблема была признана поставщиком как сохраненный XSS».

Они говорят, что обнаружили аналогичные уязвимые места на крупной бирже биткойнов, на веб-сайте крупного университета и в службе веб-почты правительства Индии.

Исследователи выявили 1,4 миллиона веб-серверов, потенциально уязвимых для подобного рода путаницы в протоколах, и 119 000 из них, которые открыты для атак со стороны сервера приложений, которым можно воспользоваться. PoC-код размещен на GitHub.

С октября прошлого года исследователи обсуждали свои выводы с различными проектами с открытым исходным кодом, такими как OpenSSL, разработчиками различных библиотек TLS, такими проектами, как nginx и Apache, а также различными проектами FTP и почтовых серверов.

Боффины утверждают, что нет причин для паники, потому что атака ALPACA требует ряда предварительных условий для работы и зависит от сложного взаимодействия между приложениями, протоколами и браузерами. В то же время нельзя игнорировать ALPACA.

Среди выявленных комбинаций уязвимых приложений и браузеров: Sendmail SMTP (Internet Explorer) через STARTTLS; Cyrus, Kerio Connect и Zimbra IMAP с поддержкой атак загрузки и отражения (Internet Explorer); Courier, Cyrus, Kerio Connect и Zimbra разрешили загрузочные атаки (Internet Explorer); Microsoft IIS, vsftpd, FileZilla Server и FTP-серверы Serv-U сделали возможными атаки отражения (Internet Explorer); и эти же FTP-серверы разрешали атаки загрузки и скачивания в любом браузере.

Предлагаемые меры включают реализацию расширений протокола Application Layer Protocol Negotiation (ALPN) и Server Name Indication (SNI) для TLS в качестве барьера для межпротокольных атак. Проблема в том, что развертывание этих средств защиты может отключить устаревшие клиенты и серверы, которые еще не были обновлены.

Исправление этой ошибки – не простой патч; скорее для этого требуются обновления нескольких библиотек и приложений. Исследователи говорят, что они ожидают, что ALPACA будет составлять нашу компанию на долгие годы». ***(Thomas Claburn. ALPACA gnaws through TLS protection to snarf cookies and steal data // The Register (https://www.theregister.com/2021/06/10/alpaca_tls_protection/). 10.06.2021).***

***

**«Команда McAfee Advanced Threat Research (ATR) обнаружила уязвимость (CVE-2021-33887) в процессе проверенной загрузки Android (AVB), который сделал Peloton уязвимым.**

По словам McAfee, продукты Peloton оснащены большим планшетом, который взаимодействует с компонентами фитнес-тренажера, а также дает возможность посещать виртуальные занятия по тренировкам через Интернет. Однако «под капотом» этого глянцевого корпуса скрывается стандартный Android-планшет. Недавно компания Peloton привлекла внимание к проблемам, связанным с конфиденциальностью и безопасностью ее продуктов.

В ATR McAfee заявили, что проблема связана с процессом загрузки Android Verified Boot, который сопровождает стационарный велотренажер Peloton Bike +. McAfee сказал, что злоумышленники могут получить доступ к байку через порт и установить поддельные версии популярных приложений, которые затем могут обмануть пользователей, введя их личную информацию. Однако для атаки потребуется физический доступ к продукту Peloton.

McAfee ATR разослала поставщику полную информацию 2 марта 2021 г. – вскоре после этого компания Peloton подтвердила наличие проблемы и впоследствии выпустила исправление для нее в версии программного обеспечения «PTX14A-290». Глава Peloton по глобальной информационной безопасности Адриан Стоун поделился следующим: «Эта уязвимость, о которой сообщает McAfee, потребует прямого физического доступа к Peloton Bike + или Tread. Как и

в случае с любым подключенным домашним устройством, если злоумышленник может получить к нему физический доступ, все большее значение приобретают дополнительные физические средства контроля и защиты. Чтобы обеспечить безопасность наших участников, мы действовали быстро и в координации с McAfee. Мы выпустили обязательное обновление в начале июня, и каждое устройство с установленным обновлением защищено от этой проблемы».

Джек Маннино, генеральный директор nVisium, поставщика безопасности приложений из Фоллс-Черч, штат Вирджиния, объясняет: «Эта проблема не уникальна для Peloton. Многие OEM-производители устройств Android страдают от аналогичных недостатков, поставляемых в производственные устройства. Android предоставляет возможности для проверенной загрузки, но параметры безопасности загрузчика по-прежнему должны быть правильно настроены производителем, иначе, как было продемонстрировано, злоумышленник может получить полный контроль над загрузчиком и устройством».

Сету Кулкарни, вице-президент по стратегии в WhiteHat Security, провайдере безопасности приложений из Сан-Хосе, Калифорния, говорит: «Было бы легко отмахнуться от этого, сказав, что этот сценарий обхода AVB маловероятен без физического доступа к устройству. Но это было бы ошибкой, потому что шаги, предпринятые исследователями, могут быть легко воспроизведены в других операционных средах, где базовой ОС для подключенного устройства является Android».

Кулкарни добавляет: «Исследователи безопасности смогли подтвердить, что существует множество элементов управления, однако не все перестановки были протестированы. Сочетания удачи, нескольких легко доступных инструментов и подробного ведения журнала было достаточно, чтобы получить root-доступ к довольно заблокированному устройству.» ***(McAfee finds vulnerability in Peloton products // BNP Media (https://www.securitymagazine.com/articles/95440-mcafee-finds-vulnerability-in-peloton-products). 17.06.2021).***

***

**«Аналитики Avanan недавно обнаружили в Документах Google вектор эксплойтов, который злоумышленники используют для доставки вредоносных фишинговых веб-сайтов жертвам.**

Злоумышленник хочет, чтобы жертва «Нажмите здесь, чтобы загрузить документ», и как только жертва нажмет на эту ссылку, она будет перенаправлена на настоящий вредоносный фишинговый веб-сайт, где их учетные данные будут украдены через другую веб-страницу, которая выглядит как портал входа в Google.

Эту атаку на самом деле довольно просто выполнить, главным образом потому, что Google выполняет большую часть работы за злоумышленников.

Хэнк Шлесс, старший менеджер по решениям безопасности компании Lookout, говорит: «Эта фишинговая кампания может быть доставлена любому пользователю независимо от того, на каком устройстве он находится. Кампании с такой гибкостью часто имеют больше шансов на успех, особенно если они поражают цель на мобильном устройстве, где труднее обнаружить фишинговые атаки. Этот инцидент показывает, насколько просто создать убедительную

фишинговую страницу. Для этого не нужно быть опытным инженером-программистом. Сочетание этой тактики с социальная инженерия может создать очень убедительную кампанию, в которой злоумышленник сможет получить личные или корпоративные учетные данные».

«Злоумышленники знают, что кража законных учетных данных – лучший способ незаметно проникнуть в инфраструктуру организации. Поскольку большинство организаций используют либо Google Workspace, либо Microsoft 365 в качестве основной платформы повышения производительности, злоумышленники создают фишинговые кампании, специально использующие эти службы. эти учетные данные и возможность входа в облачную платформу, которую они выбрали для построения своей кампании, нет предела тому, какие данные они могут извлечь», – говорит Шесс. «Популярность этих платформ означает, что данные постоянно перемещаются между неуправляемыми устройствами и самой платформой. ИТ-отделам и специалистам по безопасности необходимо реализовать стратегию безопасности конечных точек в облаке, основанную на нулевом доверии, чтобы не отставать от сегодняшнего современного ландшафта угроз.

Шлесс добавляет: «Команды также должны иметь представление о контексте, стоящем за пользователями и устройствами, когда они пытаются войти в корпоративную инфраструктуру. Обычно, когда учетные данные скомпрометированы, первая раздача заключается в том, что пользователь входит в систему из места, находящегося очень далеко от того места, где сотрудник находится. Понимание поведения пользователя таким образом, что доступ может быть заблокирован из-за аномального местоположения входа в систему, является невероятно важной частью обеспечения безопасности современной инфраструктуры».

Хакеры обходят сканеры статических ссылок, размещая свои атаки в публично известных сервисах, говорят исследователи Avanan, которые в прошлом видели это с небольшими сервисами, такими как MailGun, FlipSnack и Movable Ink, но они впервые видят это через основной сервис, такой как Google Диск / Документы.

Джозеф Карсон, главный специалист по безопасности и консультант по информационной безопасности в ThycoticCentrify, объясняет: «Одна из самых больших ошибок, которые могут сделать профессионалы в области безопасности, – это предположить, что другие сотрудники и сотрудники имеют такое же понимание хорошей кибергигиены, что и они. Честно говоря, средний работник не обучен кибергигиене и передовым методам, делая они становятся легкой добычей для киберпреступников, стремящихся быстро и легко получить доступ к сетям организации с помощью фишинговых атак или умной социальной инженерии. Обеспечивая достаточную подготовку сотрудников на всех уровнях для выявления вредоносных электронных писем и других элементарных попыток кражи учетных данных, можно стать важным шагом на пути к снижению успешности атаки или, по крайней мере, к повышению уровня оповещения. А за счет нормализации обучения в рамках корпоративной культуры организации могут помочь сохранить бдительность в отношении этих методов в долгосрочной перспективе.

Тимур Ковалев, технический директор Untangle, говорит: «Хотя намерения сотрудника могут быть хорошими, нажатие на фишинговую ссылку может открыть дверь для хакеров. В частности, для малого бизнеса последствия атаки могут быть разрушительными, а худшие случаи приводят к закрытию бизнеса. Поощрение малых предприятий к действию и расширению их технологий кибербезопасности – это хорошо. Не все малые предприятия осведомлены о рисках, а те, кто знает о рисках, не всегда иметь достаточно бюджета, чтобы инвестировать в достаточную защиту». ***(Threat actors are using Google Docs to host phishing attacks // BNP Media (https://www.securitymagazine.com/articles/95452-threat-actors-are-using-google-docs-to-host-phishing-attacks). 18.06.2021).***

***

**«Google выпустила Chrome 91.0.4472.114 для Windows, Mac и Linux, чтобы исправить четыре уязвимости системы безопасности, одна из которых представляет собой уязвимость нулевого дня высокой степени серьезности, эксплуатируемую в дикой природе.**

Эта версия, выпущенная сегодня, 17 июня 2021 года, на канале Stable Desktop, начала распространяться по всему миру и станет доступной для всех пользователей в течение следующих нескольких дней.

Google Chrome автоматически попытается обновить браузер при следующем запуске программы, но вы можете выполнить обновление вручную, выбрав «Настройки»> «Справка»> «О Google Chrome».

*Нет подробностей об атаках нулевого дня в дикой природе*

«Google знает, что эксплойт для CVE-2021-30554 существует в дикой природе», – говорится в сообщении компании.

Нулевой день вызван использованием после бесплатного использования уязвимости в API JavaScript WebGL (Web Graphics Library), который используется веб-браузерами Chrome для визуализации интерактивной 2D– и 3D-графики без использования подключаемых модулей.

Успешное использование этой уязвимости может привести к выполнению произвольного кода на компьютерах, на которых установлены неустановленные версии Chrome.

Хотя Google заявляет, что ему известно об использовании CVE-2021-30554 в дикой природе, он не поделился информацией об этих атаках.

«Доступ к сведениям об ошибках и ссылкам может быть ограничен до тех пор, пока большинство пользователей не обновят исправление», – заявили в компании.

«Мы также сохраним ограничения, если ошибка существует в сторонней библиотеке, от которой аналогичным образом зависят другие проекты, но еще не исправлена».

Google исправил еще три серьезных использования после бесплатных ошибок сегодня в компонентах Chrome Sharing, WebAudio и TabGroups, отслеживаемых как CVE-2021-30555, CVE-2021-30556 и CVE-2021-30557.

*Седьмой Chrome нулевого дня эксплуатируется в дикой природе в этом году*

Сегодняшнее обновление устраняет седьмую уязвимость нулевого дня Google Chrome, использованную в атаках в этом году, а остальные шесть перечислены ниже:

CVE-2021-21148 – 4 февраля 2021 г.

CVE-2021-21166 – 2 марта 2021 г.

CVE-2021-21193 – 12 марта 2021 г.

CVE-2021-21220 – 13 апреля 2021 г.

CVE-2021-21224 – 20 апреля 2021 г.

CVE-2021-30551 – 9 июня 2021 г.

В дополнение к этим нулевым дням, Kaspersky сообщил, что группа злоумышленников, известная как Puzzlemaker, связывает ошибки нулевого дня Chrome, чтобы выйти из песочницы браузера и установить вредоносное ПО в системах Windows.

«Как только злоумышленники используют эксплойты Chrome и Windows, чтобы закрепиться в целевой системе, модуль stager загружает и запускает более сложный дроппер вредоносных программ с удаленного сервера», – сказал Касперский.

Project Zero, команда Google по поиску ошибок нулевого дня, также представила крупномасштабную операцию, в ходе которой группа хакеров использовала 11 нулевых дней для атак на пользователей Windows, iOS и Android в течение одного года». ***(Sergiu Gatlan. Google fixes seventh Chrome zero-day exploited in the wild this year // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/google-fixes-seventh-chrome-zero-day-exploited-in-the-wild-this-year/). 17.06.2021).***

***

**«Samsung работает над исправлением множества уязвимостей, затрагивающих его мобильные устройства, которые могут быть использованы для шпионажа или для получения полного контроля над системой.**

Ошибки являются частью более крупного набора ошибок, которые были обнаружены и ответственно сообщены одним исследователем безопасности в рамках программы поощрения ошибок компании.

*Серьезные проблемы на устройствах Samsung*

С начала года Сергей Тошин – основатель компании Oversecured, специализирующейся на безопасности мобильных приложений, обнаружил более десятка уязвимостей в устройствах Samsung.

Для трех из них детали пока неясны из-за высокого риска, который они представляют для пользователей. Не вдаваясь в подробности, Тошин сказал BleepingComputer, что наименее серьезная из этих проблем может помочь злоумышленникам украсть SMS-сообщения, если они обманут жертву.

Однако два других более серьезны, поскольку они более скрытны. Их использование не требует никаких действий со стороны пользователя устройства Samsung. Злоумышленник может использовать его для чтения и / или записи произвольных файлов с повышенными разрешениями.

Неясно, когда исправления будут отправлены пользователям, потому что процесс обычно занимает около двух месяцев из-за различных испытаний исправления, чтобы убедиться, что он не вызывает других проблем.

Тошин ответственно сообщил обо всех трех уязвимостях системы безопасности и в настоящее время ожидает вознаграждения.

*Ответственное раскрытие 17 вопросов*

Только у Samsung с начала года хакер собрал около 30 000 долларов за раскрытие 14 проблем. Остальные три уязвимости в настоящее время ждут исправления.

За семь из этих уже исправленных ошибок, за которые было выплачено вознаграждение в размере 20 690 долларов, Тошин предоставляет технические подробности и инструкции по эксплуатации, подтверждающие концепцию, в сегодняшнем сообщении в блоге.

Хакер обнаружил ошибки в предустановленных приложениях на устройствах Samsung с помощью сканера Oversecured, который он создал специально для решения этой задачи.

Он сообщил о недостатках в феврале, а также опубликовал видео, демонстрирующее, как стороннее приложение получило права администратора устройства. Однако эксплойт нулевого дня имел нежелательный побочный эффект: в процессе получения повышенных привилегий все другие приложения на телефоне Android были удалены.

Ошибка была исправлена в апреле. Это повлияло на приложение Managed Provisioning и теперь отслеживается как CVE-2021-25356. За сообщение хакер получил 7000 долларов.

Тошин получил еще одну крупную награду (5460 долларов) за то, что поделился с Samsung подробностями о проблеме (CVE-2021-25393) в приложении «Настройки», которая позволила получить доступ для чтения / записи к произвольным файлам с привилегиями системного пользователя.

Третья наиболее оплачиваемая (4850 долларов США) уязвимость из этого февральского пакета позволяла записывать произвольные файлы в качестве пользователя телефонии, который имеет доступ к сведениям о звонках и сообщениям SMS / MMS.

В мае Samsung исправила большинство этих недостатков. Однако Тошин сказал BleepingComputer, что Samsung также исправила еще один набор из семи ошибок, которые он обнаружил в рамках программы вознаграждения за ошибки компании.

Они несли риски, такие как доступ для чтения / записи к контактам пользователей, доступ к SD-карте и утечка личной информации, такой как номер телефона, адрес и электронная почта.

Пользователям рекомендуется применять последние обновления прошивки от производителя, чтобы избежать потенциальных рисков для безопасности.

Тошин сообщил о более чем 550 уязвимостях за свою карьеру, заработав более 1 миллиона долларов в виде вознаграждений за ошибки через платформу HackerOne и различные программы вознаграждения за ошибки». ***(Ionut Ilascu. Hackers can exploit bugs in Samsung pre-installed apps to spy on users // Bleeping***

***Computer® (https://www.bleepingcomputer.com/news/security/hackers-can-exploit-bugs-in-samsung-pre-installed-apps-to-spy-on-users/). 10.06.2021).***

***

**«Сегодня Microsoft выпустит патч для уязвимости, затрагивающей компонент Microsoft Office MSGraph, отвечающий за отображение графики и диаграмм, который может быть использован для выполнения кода на целевой машине.**

Поскольку компонент может быть встроен в большинство документов Office, злоумышленник может использовать его для доставки вредоносных данных без использования специальных функций.

Обнаруженная как CVE-2021-31939 уязвимость безопасности является частью более широкого набора уязвимостей, которые исследователи Check Point обнаружили в MSGraph и сообщили в Microsoft.

Причина, по которой исследователи сосредоточились на тестировании MSGraph на наличие недостатков безопасности, заключается в том, что он содержит код, которому не менее 17 лет, и имеет поверхность атаки, аналогичную редактору Microsoft Equation Editor, где ошибки, исправленные в 2017 году, продолжают активно эксплуатироваться по сей день.

Подробности об уязвимости на данный момент отсутствуют, поскольку ошибка получила идентификатор только недавно. Однако сегодня Check Point отмечает в своем отчете, что CVE-2021-31939 – это использование после бесплатного использования (UAF).

Недостаток этого типа заключается в неправильном использовании динамической памяти во время работы программы и может привести к выполнению произвольного кода в системе.

По словам исследователей, проблема заключается в функции синтаксического анализа файлов MSGraph, которая «обычно используется во многих различных продуктах Microsoft Office, таких как Excel (EXCEL.EXE), Office Online Server (EXCELCNV.EXE) и Excel для OSX».

Сегодняшнее публичное раскрытие Check Point включает три других недостатка безопасности, обнаруженных в компоненте Microsoft Office MSGraph, все они были исправлены в прошлом месяце:

CVE-2021-31174 – уязвимость чтения за пределами допустимого диапазона (OOBR), приводящая к раскрытию информации в Microsoft Excel (средняя степень серьезности); влияет на MSGraph, Office Online и Microsoft Excel

CVE-2021-31178 – уязвимость целочисленного переполнения для чтения за пределами допустимого диапазона (OOBR), приводящая к раскрытию информации (средняя степень серьезности)

CVE-2021-31179 – уязвимость, связанная с повреждением памяти, приводящая к удаленному выполнению кода (высокая степень серьезности)

Все недостатки были обнаружены с помощью фаззинга – метода тестирования, при котором код подвергается бомбардировке различными входными данными для поиска ошибок и уязвимостей безопасности.

Сгенерированные таким образом исключения включают сбои и утечки памяти, которые могут привести к эксплуатации.

Исследователи говорят, что все четыре уязвимости могут быть встроены в большинство документов Office, что оставляет место для множества сценариев атак, при этом уязвимость срабатывает, когда жертва открывает вредоносный файл Office.

«В случае эксплуатации уязвимости предоставят злоумышленнику возможность выполнить вредоносный код на целях через специально созданные документы Office», – сказал Check Point BleepingComputer.

Check Point сообщила об уязвимостях в Microsoft 28 февраля, и три из них были исправлены в прошлом месяце. CVE-2021-31939 получил свой идентификатор отслеживания позже, и сегодня планируется получить исправление». ***(Ionut Ilascu. Microsoft Office MSGraph vulnerability could lead to code execution // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/microsoft-office-msgraph-vulnerability-could-lead-to-code-execution/). 08.06.2021).***

***

**«Эксперты компании BeyondTrust, занимающейся кибербезопасностью в операционных системах UNIX, Linux, Windows и macOS, опубликовала The Annual Microsoft Vulnerabilities Report 2021» («Ежегодный отчет об уязвимостях Microsoft»).**

Согласно документу, в 2020 году в решениях техногиганта ИБ-специалисты выявили 1268 уязвимостей, что является рекордным числом. В период с 2016 по 2020 год количество уязвимостей в решениях американской компании увеличилось на 181%.

Наибольшая часть проблем была обнаружена в продуктах семейства Windows — 907. Общее число выявленных критических уязвимостей составило 132. Примечательно, что большинство проблем может быть нейтрализовано путем отключения прав администратора.

Впервые на уязвимости повышения привилегий пришлось наибольшая доля от общего числа проблем в продуктах Microsoft (44%). Данное число увеличилось почти в три раза с 198 в 2019 году до 559 в 2020 году». ***(В продуктах Microsoft в 2020 году было обнаружено рекордное количество уязвимостей // SecurityLab.ru (https://www.securitylab.ru/news/521513.php). 21.06.2021).***

***

**«Instagram исправил новую уязвимость, позволявшую любому желающему просматривать архивы публикаций и историй закрытых страниц без необходимости на них подписываться.** Как пояснил обнаруживший проблему исследователь безопасности Маюр Фартаде (Mayur Fartade), «с помощью Media ID атакующий мог видеть закрытые/архивные публикации, истории, Reels и IGTV, не будучи подписанным на пользователя».

Фартаде уведомил об уязвимости команду безопасности Facebook 16 апреля 2021 года, и она выпустила исправление 15 июня. В рамках программы выплаты вознаграждений исследователь получил $30 тыс.

Хотя для осуществления атаки злоумышленник должен знать Media ID, связанный с фотографией, видео или альбомом, Фартаде продемонстрировал, как с помощью брутфорса идентификаторов создать POST-запрос к конечной точке GraphQL и получить чувствительные данные.

В результате эксплуатации уязвимости такие соответствующие Media ID данные, как «лайки», комментарии, «сохраненное», display_url и image.uri, можно было извлечь даже без подписки на атакуемого пользователя. Кроме того, атакующий мог узнать связанную с атакуемой учетной записью страницу в Facebook.

23 апреля Фартаде обнаружил еще одну уязвимость, раскрывавшую тот же набор данных, и Facebook также выпустила для нее исправление». ***(Уязвимость в Instagram позволяла просматривать закрытые страницы без подписки на них // SecurityLab.ru (https://www.securitylab.ru/news/521365.php). 17.06.2021).***

***

**«Уязвимости, которые могли позволить XSS, CSRF и захват учетных записей одним щелчком мыши в поддоменах Atlassian, были исправлены.**

В четверг Check Point Research (CPR) сообщила, что ошибки были обнаружены в онлайн-доменах поставщика программных решений, которыми пользуются тысячи корпоративных клиентов по всему миру.

Австралийский поставщик является поставщиком инструментов, включая Jira, систему управления проектами, и Confluence, платформу для совместной работы с документами для удаленных команд.

Рассматриваемые уязвимости были обнаружены на ряде веб-сайтов, поддерживаемых Atlassian, а не в локальных или облачных продуктах Atlassian.

Поддомены atlassian.com, включая партнеров, разработчиков, поддержку, Jira, Confluence и training.atlassian.com, были уязвимы для захвата аккаунта.

CPR объяснил, что код эксплойта, использующий уязвимости в поддоменах, может быть развернут через жертву, нажав на вредоносную ссылку. Затем полезная нагрузка будет отправлена от имени жертвы, а сеанс пользователя будет украден.

Уязвимые проблемы домена включали плохо настроенную политику безопасности контента (CSP), параметры, уязвимые для обхода механизма XSS, SameSite и HTTPOnly, а также слабое место, которое позволяло фиксацию файлов cookie – возможность для злоумышленников заставить пользователей использовать файлы cookie сеанса, о которых известно их для аутентификации.

Исследователи говорят, что можно было захватить учетные записи, доступные из этих поддоменов, с помощью атак с использованием межсайтовых сценариев (XSS) и подделки межсайтовых запросов (CSRF). Кроме того, уязвимые домены также позволяли злоумышленникам нарушать сеансы связи между клиентом и веб-сервером после того, как пользователь вошел в свою учетную запись.

«Всего одним щелчком мыши злоумышленник мог использовать уязвимости, чтобы захватить учетные записи и контролировать некоторые приложения Atlassian, включая Jira и Confluence», – заявили исследователи.

Разветвления этих атак включали захват учетной записи, кражу данных, действия, выполняемые от имени пользователя, и получение доступа к тикетам Jira.

Компания Atlassian была проинформирована о результатах 8 января до публичного обнародования. Исправление для затронутых доменов было развернуто 18 мая.

*Atlassian сообщил ZDNet:*

«По результатам нашего расследования указанные уязвимости влияют на ограниченный набор веб-приложений, принадлежащих Atlassian, а также на стороннюю обучающую платформу. Atlassian предоставил исправления для решения этих проблем, и ни одна из этих уязвимостей не затронула Atlassian Cloud (например, Jira или Confluence Cloud) или локальные продукты (например, Jira Server или Confluence Server)».

Исследование Atlassian было проведено CPR из-за текущих проблем, связанных с атаками на цепочки поставок, в которых злоумышленники будут нацелены на централизованный ресурс, используемый другими компаниями.

Если этот элемент может быть скомпрометирован – например, путем подделки кода обновления из-за того, что он будет отправлен клиентам в случае Codecov, – тогда можно будет охватить более широкий круг потенциальных жертв без особых усилий.

SolarWinds также является ярким примером того, насколько разрушительной может быть атака на цепочку поставок. Примерно 18 000 клиентов SolarWinds получили вредоносное обновление программного обеспечения SolarWinds Orion, которое установило бэкдор в их системы; Однако злоумышленники выбрали несколько жертв для дальнейшего взлома, включая Microsoft, FireEye и ряд федеральных агентств.

Исследователи говорят, что можно было захватить учетные записи, доступные из этих поддоменов, с помощью атак с использованием межсайтовых сценариев (XSS) и подделки межсайтовых запросов (CSRF). Кроме того, уязвимые домены также позволяли злоумышленникам нарушать сеансы связи между клиентом и веб-сервером после того, как пользователь вошел в свою учетную запись.

«Всего одним щелчком мыши злоумышленник мог использовать уязвимости, чтобы захватить учетные записи и контролировать некоторые приложения Atlassian, включая Jira и Confluence», – заявили исследователи.

Разветвления этих атак включали захват учетной записи, кражу данных, действия, выполняемые от имени пользователя, и получение доступа к тикетам Jira.

Компания Atlassian была проинформирована о результатах 8 января до публичного обнародования. Исправление для затронутых доменов было развернуто 18 мая.

*Atlassian сообщил ZDNet:*

«По результатам нашего расследования указанные уязвимости влияют на ограниченный набор веб-приложений, принадлежащих Atlassian, а также на

стороннюю обучающую платформу. Atlassian предоставил исправления для решения этих проблем, и ни одна из этих уязвимостей не затронула Atlassian Cloud (например, Jira или Confluence Cloud) или локальные продукты (например, Jira Server или Confluence Server)».

Исследование Atlassian было проведено CPR из-за текущих проблем, связанных с атаками на цепочки поставок, в которых злоумышленники будут нацелены на централизованный ресурс, используемый другими компаниями.

Если этот элемент может быть скомпрометирован – например, путем подделки кода обновления из-за того, что он будет отправлен клиентам в случае Codecov, – тогда можно будет охватить более широкий круг потенциальных жертв без особых усилий.

SolarWinds также является ярким примером того, насколько разрушительной может быть атака на цепочку поставок. Примерно 18 000 клиентов SolarWinds получили вредоносное обновление программного обеспечения SolarWinds Orion, которое установило бэкдор в их системы; Однако злоумышленники выбрали несколько жертв для дальнейшего взлома, включая Microsoft, FireEye и ряд федеральных агентств». ***(Charlie Osborne. One-click account takeover vulnerabilities in Atlassian domains patched // ZDNet (https://www.zdnet.com/article/one-click-account-takeover-vulnerability-in-atlassian-patched/). 24.06.2021).***

***

**«Amazon объявила о новом глобальном конкурсе под названием AWS BugBust, который позволит разработчикам соревноваться за поиск и исправление одного миллиона ошибок. Компания заявила, что конкурс также поможет «сократить технический долг более чем на 100 миллионов долларов».**

В своем сообщении в блоге главный защитник AWS Мартин Биби сказал, что AWS BugBust выводит концепцию устранения ошибок «на новый уровень», позволяя разработчикам создавать частные события и управлять ими, которые эффективно «геймифицируют процесс поиска и исправления ошибок в вашем программном обеспечении.»

«Многие компании-разработчики программного обеспечения, в которых я работал (включая Amazon), запускают их за несколько недель до запуска нового продукта или услуги. [AWS BugBust] включает автоматический анализ кода, встроенные списки лидеров, настраиваемые задачи и награды», – сказал Биби сказал. «AWS BugBust способствует созданию команды и предлагает дружеское соревнование по улучшению качества кода и производительности приложений. Более того, ваши разработчики могут принять участие в крупнейшем в мире испытании кода, выиграть фантастические призы и получить признание от своих коллег».

Те, кто хочет принять участие в конкурсе, могут создать событие AWS BugBust с помощью консоли Amazon CodeGuru, инструмента разработки машинного обучения, который помогает выявлять ошибки. AWS BugBust будет иметь таблицу лидеров для разработчиков, а компания будет выдавать значки достижений и возможность оплачиваемой поездки на AWS re: Invent 2021 в Лас-Вегасе.

Свами Сивасубраманян, вице-президент Amazon Machine Learning в AWS, объяснил, что сотни тысяч клиентов AWS ежедневно создают и развертывают новые функции в приложениях с высокой скоростью и управляют сложным кодом в больших объемах.

«Трудно получить время от опытных разработчиков для быстрого выполнения эффективных проверок кода, поскольку они заняты созданием, внедрением инноваций и развертыванием», – сказал Сивасубраманян. «Сегодня мы рады объявить о совершенно новом подходе, который поможет разработчикам улучшить качество кода, устранить ошибки и повысить производительность приложений, сэкономив при этом миллионы долларов на ресурсах приложений».

Возможности AWS BugBust в настоящее время доступны в регионе США – Восточная Северная Вирджиния и вскоре будут доступны в любом регионе, где предлагается Amazon CodeGuru.

Биби отметил, что будет глобальная таблица лидеров, которая будет обновляться каждый раз, когда разработчик исправляет ошибку и набирает очки. Любой разработчик, набравший 100 баллов, получит футболку AWS BugBust, а те, кто наберет 2000 баллов, выиграют куртку AWS BugBust Varsity Jacket.

Десять лучших получат билеты на AWS re: Invent. Чтобы принять участие в глобальной задаче, проекты должны быть написаны на Python или Java, поскольку это единственные языки, поддерживаемые Amazon CodeGuru.

Биби добавил, что все расходы, связанные с базовым использованием Amazon CodeGuru Reviewer и Amazon CodeGuru Profiler, бесплатны в течение 30 дней с учетной записью AWS.

«Этот 30-дневный бесплатный период применяется, даже если вы уже использовали бесплатные уровни для Amazon CodeGuru Reviewer и Amazon CodeGuru Profiler. Вы можете создать несколько событий AWS BugBust в течение 30-дневного бесплатного пробного периода», – написал Биби. «По истечении 30-дневной бесплатной пробной версии с вас будет взиматься плата за Amazon CodeGuru Reviewer и Amazon CodeGuru Profiler в зависимости от вашего использования в задаче».

Amazon включил несколько комментариев от партнеров, которые планируют привлечь сотрудников к программе, включая Belle Fleur и Miami Dade College.

«AWS BugBust Challenge станет забавным и познавательным дополнением к нашей учебной программе, чтобы помочь нашим студентам стать более уверенными в своих способностях использовать язык программирования Python и вывести свою ИТ-карьеру на новый уровень», – сказал Антонио Дельгадо, декан инженерного факультета. Технологии и дизайн в колледже Майами Дейд.

«Мы планируем использовать AWS BugBust каждый семестр в качестве платформы для наших студентов, чтобы продемонстрировать и улучшить свои навыки программирования, одновременно являясь участниками увлекательного мероприятия по устранению ошибок». ***(Jonathan Greig. Amazon launching global competition to find and fix 1 million software bugs // ZDNet (https://www.zdnet.com/article/amazon-launching-global-competition-to-find-and-fix-1-million-software-bugs/). 24.06.2021).***

***

**«Были выявлены уязвимости в стеке Bluetooth операционной системы реального времени Zephyr, что оставляет широкий спектр устройств Интернета вещей открытыми для атак – если они не обновлены до исправленной версии ОС.**

В сообщении по безопасности, выпущенном Synopsys сегодня днем, указаны восемь ключевых уязвимостей в программном стеке Zephyr Bluetooth Low Energy (BLE). Наименее серьезные из них могут привести к атаке типа «отказ в обслуживании» путем блокировки целевого устройства; наиболее серьезные допускают утечку информации или, возможно, удаленное выполнение кода.

Уязвимости, обнаруженные с помощью программного обеспечения фаззинга Synopsys Defensics, можно использовать, когда устройства находятся в режиме рекламы и принимают соединения с удаленных устройств, что подвергает риску широкий спектр гаджетов.

«Такие устройства, как смарт-часы, фитнес-трекеры или медицинские датчики (например, датчики непрерывного мониторинга глюкозы), играют периферийную роль и находятся в режиме рекламы, чтобы телефоны могли подключаться», – говорит Матиас Кархумаа, старший инженер-программист Synopsys Cybersecurity Research. Центр, сообщили The Register.

«Как правило, диапазон Bluetooth Low Energy составляет до 100 метров. Однако режим дальнего действия Bluetooth LE, который был представлен в спецификации Bluetooth 5, может обеспечивать дальность действия до 1 км».

*Нечеткое расплывание*

Кархумаа некоторое время работал над безопасностью Bluetooth. «Тема предлагаемой мной магистерской диссертации заключалась в исследовании и внедрении нового метода для обеспечения фаззинга канального уровня Bluetooth с низким энергопотреблением», – пояснил он. «В результате мы теперь сообщаем об этих уязвимостях, которые были обнаружены с помощью решения, разработанного в рамках моей магистерской диссертации.

«Fuzz-тестирование – это методология тестирования черного ящика, при которой фаззер подает преднамеренно искаженный ввод в целевую систему и отслеживает, способна ли целевая система обрабатывать ввод без сбоев или иного неправильного поведения».

Используя этот подход, Кархумаа смог обнаружить восемь ключевых уязвимостей в стеке Zephyr Bluetooth, каждую из которых можно использовать удаленно. В некоторых случаях успешная эксплуатация просто перезагружает целевое устройство, что раздражает в случае умных часов или фитнес-трекера, что потенциально опасно для медицинских устройств.

В других случаях уязвимость может привести к зависанию всего устройства до перезагрузки вручную. Есть и такие, которые позволяют раскрывать якобы защищенную информацию, хотя и всего шесть байтов за раз, что, по словам Кархумаа, затрудняет использование в качестве практической атаки для получения пароля или ключа шифрования – или даже удаленного выполнения произвольного код.

«В целом, – отметил Кархумаа, – я рекомендую организациям не тратить слишком много времени на выяснение того, действительно ли уязвимость пригодна для использования или нет. Скорее, мы работаем над тем, чтобы упростить выявление, воспроизведение и устранение ошибок. независимо от их пригодности для использования».

*Zephyr 2.6.0 рекомендуемое обновление*

Об уязвимостях было сообщено Zephyr еще в марте этого года, а исправления были добавлены в Zephyr 2.6.0 5 июня 2021 года. Те, кто использует более ранние версии Zephyr на устройствах с поддержкой Bluetooth, должны обновить сейчас – это легче сказать, чем сделать в рынок, на котором производители слишком часто отказываются от поддержки существующих продуктов в пользу создания обновленной замены.

«В целом, да, поставщики должны работать над тем, чтобы улучшить скорость доставки обновлений прошивки для устранения уязвимостей безопасности», – сказал Кархумаа по этому последнему пункту.

«Zephyr проделала отличную работу по определению своей политики безопасности, которая гарантирует, что они предоставляют обновления безопасности для своих выпусков LTS [долгосрочной поддержки] и для двух последних выпусков, не относящихся к LTS. Участники проекта Zephyr, использующие Zephyr в своих продуктах, также получают предупреждения безопасности перед уязвимости раскрываются публично».

«Bluetooth находится в эпицентре интеллектуальной связи, но это не всегда гладко, так как многие могут попасть в ловушку, даже не осознавая, что могут появиться какие-либо эксплойты», – сказал The Register Джейк Мур, эксперт ESET по кибербезопасности в Великобритании.

«Многие из нас просто подключаются к устройствам, предполагая, что Bluetooth или беспроводная связь в целом – это простой и безопасный способ связать устройства, но уязвимости программного обеспечения могут привести к таким проблемам, как подслушивание, отказ в обслуживании или даже вредоносное ПО.

«Неисправленные дыры в безопасности потенциально могут нанести ущерб устройству Bluetooth, и обновления часто не работают в процессе обновления дома или в офисе. К счастью, атаки Bluetooth требуют, чтобы злоумышленник находился всего в нескольких футах от него, что довольно редко по сравнению с другими сложные удаленные атаки, которые часто приводят к еще большим разрушениям.

«Хотя это сложно, когда так много подключено через беспроводное соединение, возможно, стоит отключить Bluetooth, когда он не используется на таких устройствах». ***(Gareth Halfacree. Zephyr OS Bluetooth vulnerabilities left smart devices open to attack // The Register (https://www.theregister.com/2021/06/22/zephyr_os_bluetooth_vulnerabilities/). 22.06.2021).***

***

**«Western Digital предупредила клиентов о критической ошибке на своих накопителях My Book Live, предупредив их отключить устройства от Интернета, чтобы защитить устройства от удаленного стирания.**

В информационном сообщении компания по хранению данных сообщила, что устройства My Book Live и My Book Live Duo «скомпрометированы из-за использования уязвимости удаленного выполнения команд» CVE-2018-18472. Эксплойт описывается как ошибка удаленного выполнения команд root, которая может быть вызвана любым, кто знает IP-адрес затронутого устройства, и в настоящее время «используется в дикой природе в июне 2021 года для команд сброса к заводским настройкам».

В настоящее время мы рекомендуем отключить My Book Live и My Book Live Duo от Интернета, чтобы защитить свои данные на устройстве.

Сообщения о проблеме появились в четверг после того, как владельцы устройств NAS обратились с жалобами на форумы поддержки Western Digital.

«Все мои данные тоже исчезли. В сообщении в графическом интерфейсе говорится, что сегодня произошел «сброс к заводским настройкам»! Я совершенно облажался без этих данных… годы этого», – написал один пользователь.

«Я хранил все свои документы на этом диске. Все файлы пропали», – сказал другой.

Журналы устройств, опубликованные на форумах Western Digital, показывают, что устройства были сброшены к заводским настройкам удаленно, хотя виновные не были обнаружены. В заявлении, сделанном ранее сегодня, компания заявила, что не верит, что ее собственные серверы были скомпрометированы.

Western Digital My Book Live подключается к главному компьютеру через USB, а доступ в Интернет осуществляется через порт Ethernet на задней панели. Удаленный доступ осуществляется через собственные облачные серверы Western Digital.

Накопители NAS не раз становились жертвами злоумышленников. В апреле тайваньский гигант хранения данных QNAP призвал клиентов обновить свои диски перед лицом двух специально нацеленных штаммов программ-вымогателей, Qlocker и eCh0raix.

В прошлом году власти США и Великобритании предупредили о массовом заражении вредоносным ПО для кражи данных, нацеленным на диски QNAP. Атака, получившая название Qsnatch, скомпрометировала примерно 62 000 устройств. Оказавшись внутри, вредоносная программа открыла несколько бэкдоров, включая SSH и веб-оболочку, и сопротивлялась попыткам владельца развернуть обновления прошивки, которые могли бы решить проблему.

Аналогичным образом в прошлом Lenovo была поймана со спущенными штанами, спешно выпустив в 2019 году исправление прошивки для своих запоминающих устройств под брендом Iomega после того, как брешь в безопасности потенциально могла увидеть содержимое дисков, доступных в Интернете.

Хотя подробностей о том, «как» и «почему» этого конкретного инцидента пока нет, Western Digital отметила, что ее устройства My Book Live NAS последний

раз обновлялись прошивкой в 2015 году. На практике это означает почти семь лет существования уязвимостей в системе безопасности, которые не были исправлены, что подвергает пользователей риску.

Хотя Western Digital не раскрывает масштаб проблемы, быстрый поиск на Shodan показывает, что более 200 устройств My Book Live общедоступны из Интернета…». ***(Matthew Hughes. Pull your Western Digital My Book Live NAS off the internet now if you value your files // The Register (https://www.theregister.com/2021/06/25/western_digital_nas_wiped/). 25.06.2021).***

***

**«Критическая ошибка безопасности в Cortex XSOAR Palo Alto Networks может позволить удаленным злоумышленникам запускать команды и автоматизацию в Cortex XSOAR War Room и выполнять другие действия на платформе без необходимости входа в систему.**

Ошибка (CVE-2021-3044), обнаруженная внутри компании Palo Alto, представляет собой уязвимость с ненадлежащей авторизацией, которая «позволяет удаленному неаутентифицированному злоумышленнику с сетевым доступом к серверу Cortex XSOAR выполнять несанкционированные действия через REST API», согласно данным службы безопасности. Консультативный вторник продавца. По шкале критичности уязвимости CVSS он получил 9,8 из 10 возможных.

*Ошибка Cortex XSOAR: влияние на безопасность*

Согласно веб-сайту Пало-Альто, Cortex XSOAR – это платформа защиты от кибербезопасности, которая используется в различных сценариях использования, включая автоматизацию операций безопасности, управление данными об угрозах, автоматическое исправление программ-вымогателей и оркестровку облачной безопасности. SOAR расшифровывается как «управление безопасностью, автоматизация и реагирование», а в случае Пало-Альто этот термин используется для обозначения единого подхода к централизации аналитики угроз и предупреждений безопасности по источникам. Платформа Cortex также реализует автоматизированные рабочие процессы и сценарии реагирования, а также позволяет сотрудничать между командами в режиме реального времени.

Таким образом, это связующее звено с ответными мерами безопасности компании.

Если удаленные злоумышленники могут запускать команды и автоматизацию в Военной комнате, они потенциально могут подорвать текущие расследования безопасности, украсть информацию о планах действий киберзащиты жертвы и многое другое. Согласно онлайн-документации Пало-Альто, расследования в реальном времени облегчаются через War Room, что позволяет аналитикам (а в случае уязвимых систем удаленным злоумышленникам) делать следующее:

Выполняйте действия по обеспечению безопасности в реальном времени через интерфейс командной строки, не переключая консоли.

Запускайте сценарии безопасности, сценарии и команды.

Сотрудничайте и выполняйте удаленные действия в интегрированных продуктах.

Захватите контекст инцидента из разных источников.

Документируйте все действия в одном источнике.

Общайтесь с другими для совместных расследований.

«Когда вы открываете War Room, вы можете увидеть ряд записей, таких как команды, заметки, доказательства, задачи и т. Д.», – говорится в документации.

Однако смягчающим фактором является тот факт, что злоумышленник, как уже упоминалось, должен иметь доступ к той же сети, к которой подключен Cortex XSOAR, что требует более раннего взлома или использования уязвимости.

Затронутые версии и исправления

Проблема затрагивает только конфигурации Cortex XSOAR с активной интеграцией ключей API, и в частности следующие версии: Cortex XSOAR 6.1.0 строится позже, чем 1016923 и ранее, чем 1271064; и Cortex XSOAR 6.2.0 построены ранее, чем 1271065.

Чтобы обезопасить себя, пользователи должны обновиться до последней версии.

Пало-Альто сказал, что ему ничего не известно об использовании этой ошибки в дикой природе». ***(Tara Seals. Critical Palo Alto Cyber-Defense Bug Allows Remote 'War Room' Access // Threatpost (https://threatpost.com/critical-palo-alto-bug-remote-war-room/167169/). 23.06.2021).***

***

**«По словам исследователей, серия из четырех уязвимостей высокой степени опасности может позволить удаленным злоумышленникам выполнить произвольный код в предзагрузочной среде на устройствах Dell. По оценкам, они затрагивают около 30 миллионов отдельных оконечных устройств Dell по всему миру.**

Согласно анализу Eclypsium, ошибки затрагивают 129 моделей ноутбуков, планшетов и настольных компьютеров, включая корпоративные и потребительские устройства, которые защищены функцией безопасной загрузки. Безопасная загрузка – это стандарт безопасности, направленный на то, чтобы устройство загружалось с использованием только программного обеспечения, которому доверяет производитель оригинального оборудования (OEM), чтобы предотвратить несанкционированный захват.

Как сообщили в четверг исследователи Eclypsium, эти ошибки позволяют привилегированным сетевым злоумышленникам обходить защиту безопасной загрузки, контролировать процесс загрузки устройства и подрывать операционную систему и средства контроля безопасности более высокого уровня. Они имеют совокупный балл по CVSS 8,3 из 10.

В частности, проблемы затрагивают функцию BIOSConnect в Dell SupportAssist (решение технической поддержки, которое предустановлено на большинстве компьютеров Dell под управлением Windows). BIOSConnect используется для удаленного восстановления ОС или для обновления прошивки устройства.

«Поставщики технологий всех типов все чаще внедряют процессы обновления по беспроводной сети, чтобы максимально упростить для своих клиентов обновление встроенного ПО и восстановление после сбоев системы», –

отмечают исследователи в анализе. «И хотя это ценный вариант, любые уязвимости в этих процессах, подобные тем, которые мы видели здесь в BIOSConnect от Dell, могут иметь серьезные последствия».

В отчете отмечается, что конкретные уязвимости позволяют злоумышленнику удаленно использовать прошивку UEFI хоста и получить контроль над наиболее привилегированным кодом на устройстве.

«Такое сочетание возможности удаленного использования и высоких привилегий, вероятно, сделает функцию удаленного обновления привлекательной целью для злоумышленников в будущем», – говорится в отчете.

*Небезопасное соединение TLS: выдача себя за Dell*

Первая уязвимость (CVE-2021-21571) – это начало цепочки, которая может привести к удаленному выполнению кода (RCE).

Когда BIOSConnect пытается подключиться к внутреннему HTTP-серверу Dell для выполнения удаленного обновления или восстановления, он позволяет BIOS системы (микропрограммному обеспечению, используемому для инициализации оборудования во время процесса загрузки) обращаться к серверным службам Dell через Интернет. Затем он координирует процесс обновления или восстановления.

По словам исследователей Eclypsium, проблема в том, что соединение TLS, используемое для подключения BIOS к внутренним серверам, будет принимать любой действительный сертификат с подстановочными знаками. Таким образом, злоумышленник с привилегированным положением в сети может перехватить это соединение, выдать себя за Dell и доставить контролируемый злоумышленником контент обратно на устройство жертвы.

«Процесс проверки сертификата для dell.com выполняется путем получения записи DNS с жестко запрограммированного сервера 8.8.8.8, а затем установления соединения с [сайтом загрузки Dell]», – говорится в анализе. «Однако любой действительный шаблонный сертификат, выданный любым из встроенных центров сертификации, содержащихся в функции BIOSConnect в BIOS, будет удовлетворять условию безопасного соединения, и BIOSConnect продолжит извлечение соответствующих файлов. Пакет корневых сертификатов ЦС в образе BIOS был получен из файла корневого сертификата Mozilla (certdata.txt)».

*Уязвимости переполнения, обеспечивающие выполнение произвольного кода*

Как только эта первая ошибка «привратника» используется для доставки вредоносного контента обратно на машину жертвы, у злоумышленников есть выбор из трех отдельных и независимых уязвимостей переполнения (CVE-2021-21572, CVE-2021-21573, CVE-2021-21574)., по словам исследователей, любой из них можно использовать для получения RCE перед загрузкой на целевом устройстве.

Две уязвимости влияют на процесс восстановления ОС, а третья влияет на процесс обновления прошивки, согласно Eclypsium, которая пока не раскрывает дальнейшие технические подробности.

Любой сценарий атаки потребует от злоумышленника возможности перенаправить трафик жертвы, например, с помощью атаки «машина посередине» (MITM) – что, по словам исследователей, не является большим препятствием.

«Атаки типа «машина посередине» – относительно низкая планка для изощренных злоумышленников, при этом такие методы, как подмена ARP и отравление кеша DNS, хорошо известны и легко автоматизируются», – говорится в отчете. «Кроме того, корпоративные VPN и другие сетевые устройства стали главной целью злоумышленников, и недостатки в этих устройствах могут позволить злоумышленникам перенаправить трафик. И, наконец, конечные пользователи, работающие из дома, все больше полагаются на сетевое оборудование SOHO. Уязвимости довольно часто встречаются в сетевых устройствах потребительского уровня и используются в широкомасштабных кампаниях».

Фундаментальные усилия по проведению атаки, вероятно, являются положительным компромиссом для киберпреступников, учитывая, что успешная компрометация BIOS устройства позволит злоумышленникам обеспечить постоянное постоянство, контролируя при этом наивысшие привилегии на устройстве. Это связано с тем, что они будут контролировать процесс загрузки операционной системы хоста и смогут отключить защиту, чтобы оставаться незамеченными, отмечается в отчете.

«Практически неограниченный контроль над устройством, который может обеспечить эта атака, оправдывает свои усилия для злоумышленника», – заявили исследователи Eclypsium.

*Исправления ошибок Dell*

Dell выпустила исправления для BIOS на всех затронутых системах. Для получения подробной информации обратитесь к его рекомендациям.

«Рекомендуется запускать исполняемый файл обновления BIOS из ОС после ручной проверки хэшей с хешами, опубликованными Dell», – рекомендовал Eclypsium, вместо того, чтобы полагаться на BIOSConnect для применения обновлений BIOS». ***(Tara Seals. 30M Dell Devices at Risk for Remote BIOS Attacks, RCE // Threatpost (https://threatpost.com/dell-bios-attacks-rce/167195/). 24.06.2021).***

***

**«Исследователи обнаружили, что Atlassian, платформу, используемую 180 000 клиентов для разработки программного обеспечения и управления проектами, могла быть взломана одним щелчком мыши из-за недостатков безопасности.**

В четверг Check Point Research (CPR) опубликовала отчет (PDF), в котором описывается, как злоумышленник мог использовать ошибки для доступа к Atlassian Jira: проприетарному инструменту отслеживания ошибок и гибкого управления проектами. Среди поклонников Jira есть немало тяжеловесов: инструмент для разработки программного обеспечения используют более 65 000 клиентов, в том числе такие, как Apache Software Foundation, Cisco, Fedora Commons, Hibernate, Pfizer и Visa.

Исследователи CPR заявили, что всего одним щелчком мыши злоумышленник мог перекачать конфиденциальную информацию из Jira.

Автор отчета Роман Заикин, исследователь CPR, сказал Threatpost, что основная проблема связана с платформой Atlassian: команда «нашла несколько

уязвимостей и связала их, чтобы найти эту ошибку», – сказал он. Что касается того, какая конфиденциальная информация могла быть выведена из платформы, Заикин сказал, что она будет включать «все, что связано с управлением командой или написанием… кода, в котором вы можете столкнуться с ошибками».

Недостатки также могли позволить злоумышленнику захватить учетные записи и контролировать некоторые приложения Atlassian, включая Jira и Confluence, корпоративную веб-вики, которая поставляется со встроенным веб-сервером Tomcat и базой данных hsql, а также поддерживает другие базы данных. Более 60 000 клиентов используют Confluence, в том числе LinkedIn, NASA и New York Times.

*Атака цепочки поставок в стиле SolarWinds*

При таком уровне контроля над Atlassian можно представить себе потенциальный эксплойт, который был бы похож на атаку цепочки поставок SolarWinds, в которой злоумышленники использовали пароль по умолчанию как открытую дверь в механизм обновления программного обеспечения.

Злоумышленники в этой масштабной кампании смогли использовать платформу управления сетью Orion компании SolarWinds для заражения целей, запустив специальный бэкдор под названием Sunburst через троянизированные обновления продукта. На самом деле масштабность – это преуменьшение: атака цепочки поставок позволила скомпрометировать главу Министерства внутренней безопасности (DHS) при бывшем президенте Трампе, других высокопоставленных сотрудников отдела кибербезопасности, многочисленные крупные предприятия и другое правительство США. агентства.

Следует отметить, что Orion – это инструмент для мониторинга и управления инфраструктурой, который находится в зоне наилучшего восприятия сети, где он достигает других активов и, таким образом, представляет собой идеальный базовый лагерь для злоумышленника для выполнения других вредоносных действий.

Фактически, именно катастрофа SolarWinds вдохновила CPR исследовать Atlassian в первую очередь: исследователи заявили, что после инцидента у них возникло любопытство по поводу атак на цепочки поставок.

В ходе расследования CPR удалось обойти меры безопасности Atlassian, «доказав, что злоумышленник мог внедрить вредоносный код, выполнить действия от имени пользователей и захватить пользовательские сеансы», – пишут исследователи CPR.

Они отметили, что Bitbucket, служба хостинга репозитория исходного кода на основе Git, также могла сыграть роль в атаке на цепочку поставок, нацеленной на партнеров и клиентов Atlassian. Уязвимость затронула несколько поддерживаемых Atlassian веб-сайтов, которые поддерживают клиентов и партнеров, но не затрагивают облачные или локальные продукты Atlassian.

Одед Вануну, руководитель отдела исследований уязвимостей продуктов в CPR, цитируется в пресс-релизе, говоря, что атаки на цепочки поставок «вызывали у нас интерес весь год, начиная с инцидента с SolarWinds». Он отметил, что платформы Atlassian занимают «центральное место в рабочем процессе организации».

«Невероятное количество информации о цепочке поставок проходит через эти приложения, а также через проектирование и управление проектами», – продолжил Вануну. «Следовательно, мы начали задавать несколько провокационный вопрос: какую информацию может получить злоумышленник, если он войдет в учетную запись Jira или Confluence?»

*Захват аккаунта*

Ответ: много конфиденциальной информации. В своих исследованиях CPR добился перехвата учетных записей Atlassian, доступных через поддомены atlassian.com. Вот поддомены, которые исследователи сочли уязвимыми:

jira.atlassian.com
confluence.atlassian.com
getsupport.atlassian.com
partners.atlassian.com
developer.atlassian.com
support.atlassian.com
training.atlassian.com

Эти ошибки позволили бы злоумышленнику составить обширный список вредоносных действий, таких как атаки с использованием межсайтовых сценариев (XSS); атаки с подделкой межсайтовых запросов (CSRF); или атаки фиксации сеанса.

«Другими словами, злоумышленник может использовать недостатки безопасности, обнаруженные CPR, чтобы получить контроль над учетной записью жертвы, выполнить действия от его имени и получить доступ к тикетам Jira», – отметили исследователи. «Кроме того, злоумышленник мог редактировать вики-страницу Confluence компании или [просматривать] тикеты на GetSupport. Злоумышленник мог продолжить получение личной информации. Все это можно сделать одним щелчком мыши».

Для использования Atlassian требовалось, во-первых, найти способ внедрить код в Atlassian. Исследователи сделали это с помощью XSS-уязвимости на поддомене «training.atlassian.com», который предлагает пользователям курсы или кредиты. Когда тип элемента – «training_credit», добавляется дополнительный параметр «options._training_credit_account», чтобы запросить параметр, который был уязвим для XSS.

Исследователи объяснили, что политика безопасности контента (CSP) была «плохо настроена» на этом поддомене с помощью директив «unsafe-inline» и «unsafe-eval», что позволяет выполнять скрипт. По их словам, это сделало субдомен «идеальной отправной точкой» для исследования. Они смогли использовать ошибку XSS, чтобы перехватить все файлы cookie и локальное хранилище цели.

Затем, поскольку сохраненный XSS-файл можно было запустить только при добавлении товаров в корзину, исследователи попытались выяснить, могут ли они заставить пользователя добавить вредоносный элемент без уведомления пользователя. Учитывая, что токена CSRF не было, они могли выполнить CSRF-атаку на список покупок и выполнить свою полезную нагрузку. Для этого они загрузили доказательство концепции и отправили его потенциальной жертве.

Поскольку эта полезная нагрузка была сохранена XSS, она была сохранена в базе данных и добавлена в список покупок, а их вредоносный элемент был добавлен в корзину.

Исследователи использовали эту инъекцию кода, чтобы добавить новый файл cookie сеанса в учетную запись пользователя, и в сочетании с уязвимостью фиксации сеанса в доменах Atlassian им удалось захватить учетные записи.

*Методология атаки*

Успешная цепочка атак повлекла бы за собой следующие шаги:

Злоумышленник побуждает жертву щелкнуть созданную ссылку (исходящую из домена Atlassian) либо из социальных сетей, либо из поддельного электронного письма, либо из приложения для обмена сообщениями и т. Д.

При нажатии на ссылку полезная нагрузка отправляет запрос от имени жертвы на платформу Atlassian, которая бы выполнила атаку и украла сеанс пользователя.

Злоумышленник входит в приложения жертвы Atlassian, связанные с учетной записью, получая всю конфиденциальную информацию, хранящуюся в нем.

CPR представила Atlassian результаты своих исследований 8 января. По словам исследователей CPR, Atlassian заявила, что развернула исправление 18 мая…» ***(Lisa Vaas. Atlassian Bugs Could Have Led to 1-Click Takeover // Threatpost (https://threatpost.com/atlassian-bugs-could-have-led-to-1-click-takeover/167203/). 24.06.2021).***

***

**«Хакеры сканируют и активно используют уязвимости в устройствах Cisco ASA после того, как PoC-эксплойт был опубликован в Twitter.**

Эта уязвимость Cisco ASA представляет собой уязвимость межсайтового сценария (XSS), которая отслеживается как CVE-2020-3580.

Cisco впервые раскрыла уязвимость и выпустила исправление в октябре 2020 года. Однако первоначальное исправление для CVE-2020-3580 было неполным, и дополнительное исправление было выпущено в апреле 2021 года.

Эта уязвимость может позволить неаутентифицированному злоумышленнику отправлять целевые фишинговые электронные письма или вредоносные ссылки пользователю устройства Cisco ASA для выполнения команд JavaScript в браузере пользователя.

«Успешный эксплуатируют может позволить злоумышленнику выполнить произвольный код сценария в контексте интерфейса или позволить злоумышленнику получить доступ к конфиденциальной основе браузера информации,» говорят Cisco, рекомендательные.

*Хакеры используют недавно опубликованный эксплойт PoC*

После того, как уязвимость была исправлена и было дано достаточно времени для обновления устройств, исследователи безопасности обычно публикуют экспериментальные эксплойты (PoC), чтобы рассказать, как организации обнаруживают и предотвращают связанные атаки.

В четверг исследователи из Positive Technologies Offensive Team опубликовали PoC-эксплойт для уязвимости Cisco ASA CVE-2020-3580 в Twitter.

Выпущенный эксплойт будет отображать предупреждение JavaScript в браузере пользователя, когда он посещает специально созданную вредоносную веб-страницу. Однако вредоносная веб-страница могла выполнять другие команды JavaScript для выполнения вредоносных действий.

Вскоре после того, как PoC был выпущен, Tenable сообщила, что злоумышленники активно используют уязвимость на уязвимых устройствах, но не раскрыла, какие вредоносные действия выполнялись.

«Tenable также получила сообщение о том, что злоумышленники эксплуатируют CVE-2020-3580 в «дикой природе», – сказал Тенабл.

Поскольку злоумышленники сейчас активно используют уязвимость, администраторам крайне важно немедленно исправить уязвимые устройства Cisco ASA, чтобы злоумышленники не могли их использовать». ***(Lawrence Abrams. Cisco ASA vulnerability actively exploited after exploit released // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/cisco-asa-vulnerability-actively-exploited-after-exploit-released/). 27.06.2021).***

***

**«На этой неделе приложение VMware Carbon Black App Control было обновлено, чтобы исправить критическую уязвимость, которая позволяет получить доступ к серверу без аутентификации.**

Carbon Black App Control разработан для корпоративных сред, чтобы усилить безопасность систем, как старых, так и новых, и защитить их от несанкционированных модификаций, например, созданных вредоносными программами или эксплойтами нулевого дня.

*Путь к разблокировке критических систем*

Уязвимость, отслеживаемая как CVE-2021-21998, представляет собой обход аутентификации, затрагивающий VMware Carbon Black App Control (AppC) версий 8.0, 8.1, 8.5 до 8.5.8 и 8.6 до 8.6.2.

Злоумышленники, имеющие доступ к серверу управления AppC, могут использовать ошибку, чтобы получить административные привилегии без необходимости аутентификации, говорится в рекомендациях по безопасности от VMware.

Учитывая роль продукта в корпоративной сети, получение контроля над сервером управления AppC открывает путь к компрометации критически важных систем.

В зависимости от среды злоумышленник может использовать уязвимость для нацеливания на что угодно, от точек продаж (PoS) до промышленных систем управления.

Оценка серьезности уязвимости была рассчитана до 9,4, что делает ее критической проблемой, которой пользователи и администраторы должны уделять приоритетное внимание.

Обходных путей нет, и проблему можно решить, установив исправление, доступное для AppC 8.1.x и 8.0.x, или обновив продукт до версии 8.6.2 или 8.5.8.

*Запуск кода с повышенными привилегиями*

Помимо исправления CVE-2021-21998, VMware также исправила локальную ошибку повышения привилегий, затрагивающую VMware Tools для Windows, VMware Remote Console для Windows (VMRC для Windows) и VMware App Volumes.

Недостаток обозначен как CVE-2021-21999. В настоящее время у него нет оценки степени серьезности от Национального института стандартов и технологий (NIST), но VMware оценила ее на 7,8 (высокая степень серьезности).

За обнаружение и сообщение о CVE-2021-21999 приписываются Зишан Шейх из NotSoSecure, работающий с Trend Micro Zero Day Initiative (ZDI), и Хоу ЦзинИ из Qihoo 360.

CISA также выпустила рекомендацию, чтобы побудить пользователей и сетевых администраторов ознакомиться с последними инструкциями по безопасности от VMware и применить обновления». ***(Ionut Ilascu. VMware fixes authentication bypass in Carbon Black App Control // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/vmware-fixes-authentication-bypass-in-carbon-black-app-control/). 23.06.2021).***

***

## *Технічні та програмні рішення для протидії кібернетичним загрозам*

---

**«Softprom расширил свой портфель ИТ-безопасности флагманским решением по кибербезопасности Cyberquest компании Nextgen Software.** В соответствии с дистрибьюторским соглашением Softprom будет продвигать решения данного разработчика в регионе СНГ, на Кавказе и в ряде европейских стран, включая Албанию, Армению, Австрию, Боснию и Герцеговину, Болгарию, Хорватию, Кипр, Чехию, Эстонию, Грузию, Германию, Грецию, Венгрию, Косово, Латвию, Литву, Черногорию, Северную Македонию, Польшу, Сербию, Словакию, Словению и Швейцарию.

Как отмечается, платформа для анализа безопасности больших данных Cyberquest представляет собой коллаборацию коллектива людей с обширным отраслевым опытом проектирования и разработки, а также внедрения решений по кибербезопасности.

«Cyberquest как платформа NextGen SIEM обеспечивает максимально привлекательное соотношение цены и качества, достойное внимания многих компаний, и мы рады предложить это решение нашим партнерам», – сказал Павел Жданович, управляющий директор Softprom». ***(Аналитическая платформа Cyberquest пополнила портфель решений ИТ-безопасности Softprom // Компьютерное Обозрение (https://ko.com.ua/analiticheskaya_platforma_cyberquest_popolnila_portfel_reshenij_it-bezopasnosti_softprom_137568). 02.06.2021).***

***

**«Компания Immersive Labs, занимающаяся подготовкой к кибербезопасности, объявила о раунде серии C на сумму 75 миллионов долларов с инвестициями от Citi Ventures, Menlo Ventures и последующей деятельности от Goldman Sachs Asset Management.**

Компания помогает организациям анализировать свою кибербезопасность «среди технических и нетехнических команд», а также предоставляет инструменты для улучшения кибер-обучения. Immersive Labs теперь продает новую платформу «Оптимизация кибербезопасности», которая будет стремиться предоставлять ряд услуг, связанных с выявлением пробелов в кибербезопасности на предприятии.

«От антикризисного управления с руководителями до обеспечения разработки программного обеспечения инженерами и обеспечения соответствия в юридических группах – платформа будет использовать аналитические данные, чтобы понять, где требуются навыки, и внедрить обучение для конкретных ролей», – говорится в заявлении компании о своих услугах. «Это также позволит использовать показатели и бенчмаркинг на уровне совета директоров».

Компания уже получила 48 миллионов долларов венчурного финансирования, и платформа используется в таких компаниях, как Vodafone и HSBC, а также в таких организациях, как NHS в Великобритании.

«Хотя технологии традиционно использовались, чтобы восполнить этот пробел, они неспособны принимать тонкие решения, мыслить нестандартно, прививать культуру, демонстрировать лидерство или принимать во внимание множество других важных факторов», – сказал ZDNet Джеймс Хэдли, генеральный директор Immersive Labs.

«Мы считаем, что человеческий интеллект заслуживает того, чтобы занять свое место рядом с искусственным интеллектом в кибербезопасности, чтобы помочь организациям повысить устойчивость и снизить риски».

Хэдли сказал, что знания и навыки в области кибербезопасности больше не должны быть «прерогативой нескольких технических специалистов, спрятанных в бэк-офисе».

Он добавил, что новое финансирование позволит компании добавить «новые аналитические возможности и контент, чтобы предоставить более подробную картину навыков по растущей широте и глубине кибер-уязвимости, с которой сталкиваются организации, что поможет им лучше измерять риски и управлять ими».

По его словам, киберзнания, навыки и возможности становятся все более востребованными во всех организациях, и не только группам безопасности требуется постоянное повышение квалификации, но и разработчикам необходимо знать, как писать безопасный код, а командам нужно нанимать подходящих специалистов.

«Это создает потребность в навыках как технических, так и нетехнических команд, чтобы идти в ногу с атакующими. Для этого сначала вам нужно понять, где находятся эти пробелы. Наша платформа способна собирать эту информацию, используя наши собственные – среды онлайн-обучения, в которых люди участвуют в сценариях и упражнениях по кибербезопасности, охватывающих все темы и роли, от генерального директора, участвующего в атаке программы-вымогателя со всей

своей командой, до передового аналитика, индивидуально перепроектирующего вредоносное ПО», – пояснил Хэдли.

«Собирая информацию о том, кто и когда был повышен квалификация против каких угроз, специфичных для их роли, и сравнивая ее с метаданными, мы можем предоставить общее представление о возможностях навыков».

Платформа предлагает учебные занятия и игровую среду, чтобы помочь заполнить любые пробелы в навыках, обнаруженные в процессе анализа.

«Это гораздо более рентабельный и эффективный способ обучения, ускоряющий цикл навыков таким образом, чтобы это было более актуально для сегодняшней удаленной рабочей силы и существующей угрозы. Это также позволит директорам по информационным технологиям отчитываться об уровнях квалификации перед советом директоров. чтобы сделать их большей частью общей киберустойчивости бизнеса», – добавил Хэдли.

«В основе нашей платформы лежат лаборатории и сценарии кризисов: игровые упражнения, основанные на сюжетах, доступные по запросу через браузер и подходящие для различных ролей и технических возможностей. Они основаны на аналитике новых угроз и составлены нашей командой штатных экспертов, которые специализируются во всем: от кибер-кризисов до безопасности приложений и шифрования. Новые лаборатории создаются постоянно, иногда в течение нескольких часов после появления новой угрозы».

Компания будет использовать недавний приток финансирования для расширения своего присутствия на международном уровне и довести глобальную численность персонала до 600 человек в течение следующих двух лет. Планируется также создание региональных операционных центров в Европе и Азиатско-Тихоокеанском регионе.

В настоящее время штаб-квартиры компании находятся в Бостоне и Бристоле, а общее количество сотрудников составляет около 200 человек.

Венки Ганесан, партнер Menlo Ventures, сказал, что нехватка рабочей силы в сфере кибербезопасности заставляет организации информировать каждого сотрудника о последних угрозах.

«Immersive Labs помогает крупным организациям противостоять этой проблеме, сочетая интеллектуальный анализ данных с целевым обучением. Угроза кибербезопасности будет только возрастать, что делает Immersive Labs перспективными в будущем, поскольку они стремятся помочь крупным предприятиям обучаться и защищать себя от постоянно развивающихся угроз», – сказал он. – сказал Ганешан.

Другие инвесторы, такие как Арвинд Пурушотхам из Citi Ventures, поддержали эти идеи, отметив, что работа Immersive Labs «создает видимость и оптимизирует один из самых ценных активов в киберзащите – человеческих защитников». ***(Jonathan Greig. Cyber resilience company Immersive Labs announces $75 million Series C round // ZDNet (https://www.zdnet.com/article/cyber-resilience-company-immersive-labs-announces-75-million-series-c-round/). 14.06.2021).***

***

**«Энтропия – это термин, используемый для статистической неопределенности части данных, одним из примеров которой являются случайно сгенерированные числа, которые используются в криптографических ключах и которые трудно взломать до такой степени, что такие строки действительно трудно для компьютера предсказывает.**

Утверждая, что сегодняшнее шифрование недостаточно непредсказуемо, стартап Qrypt из Нью-Йорка в среду официально объявил о своем намерении предложить «энтропию как услугу» или EaaS, чтобы предоставить предприятиям, а также частным лицам возможность генерации действительно случайных чисел. возможности.

«У каждого есть неотъемлемое право на неприкосновенность частной жизни; мы считаем, что это право подвергается нападкам со стороны России, Китая и любого злоумышленника, которого вы хотите выбрать», – сказал основатель и генеральный директор Кевин Чалкер в интервью ZDNet через Zoom.

Основное утверждение Qrypt заключается в том, что текущий режим криптографических инструментов, основанный на таких вещах, как алгоритм RSA и обмен публично-частным ключом, уже уязвим, потому что возможности генерации псевдослучайных чисел такой сети могут быть взломаны с помощью достаточной вычислительной мощности.

В будущем квантовые вычисления должны обладать достаточной мощностью, чтобы регулярно взламывать псевдослучайный код – надвигающийся риск, который уже широко обсуждался как исчезновение традиционных криптографических инструментов.

В случаях, когда коды не могут быть взломаны в данный момент, злоумышленники, которые крадут данные, будут размещать эти данные в зашифрованном виде на диске в качестве урожая в ожидании того дня, когда станут доступны квантовые инструменты для дешифрования данных.

Вдохновение исходит от одноразовых генераторов криптографических шифров, используемых для тайных операций. Хотя полная информация о подходе Qrypt все еще несколько ограничена, в основном Qrypt сотрудничает с частной компанией Quside Technologies, расположенной в Барселоне, для генерации случайных чисел на основе квантов.

Quside, созданный на базе Барселонского Института фотонных наук, использует полупроводниковые лазеры для создания интерференционных картин, которые можно дискретизировать для получения случайного числа.

Таким образом, выборка реального физического процесса, такого как интерференционная картина фотонов, обычно считается наиболее безопасным способом получения действительно случайного «начального числа» для генератора случайных чисел. Квантовая природа такого измерения считается более случайной, чем бросание матрицы, которое является классической механической операцией.

Qrypt EaaS, используя устройства, соединенные вместе распределенным образом, берет начальное число Quside и использует его для генерации так называемого источника энтропии, необработанной случайности, которую затем можно использовать для создания одноразового блокнота на компьютерах каждой взаимодействующей стороны. любой конец незащищенной линии связи.

Сервис является альтернативой квантовому распределению ключей или QKD.

Если сеть QKD имеет два устройства-генератора ключей, подключенных через надежную линию связи, сеть Qrypt EaaS распределяет необработанные случайные источники в цифровом виде среди пользователей распределенным образом, а затем запускает так называемый алгоритм BLAST, который одновременно генерирует одноразовые контактные данные. на обоих концах связи.

Алгоритм BLAST был разработан Евгением Додисом, главным криптографом фирмы, сотрудником Международной ассоциации криптологических исследований и имеющим множество публикаций по таким методам, как обмен ключами.

Генеральный директор Чалкер ранее был «оперативным сотрудником» ЦРУ, тайным оперативником на местах в рамках так называемых подпольных служб, сосредоточенных на Иране. Главным техническим директором Qrypt является Денис Мандич, также ранее работавший в ЦРУ, также являющийся секретным агентом, сосредоточенным на России.

Оба человека подчеркивают, что Qrypt EaaS предназначен для предоставления розничному / потребительскому рынку такого же уровня криптографической стойкости для безопасного обмена сообщениями и других приложений.

«Мы пытаемся демократизировать тот же уровень безопасности, на который мы полагались все эти годы», – сказал Чалкер.

«Мы можем сделать это прямо сейчас с коммерческой готовой инфраструктурой, вам не нужно строить что-то новое, полностью цифровое, отсюда на другой конец света», – сказал Мандич.

Существующее шифрование, отмечает Мандич, можно взломать даже без кванта, особенно в случаях неэффективного использования одноразовых блокнотов. «Если вы повторно используете одноразовые прокладки или у вас нет действительно случайных одноразовых прокладок, они станут ломкими».

По словам Мандича, устройства Qrypt размещаются в центрах обработки данных по всему миру, «географически и политически распределенных».

До сих пор Qrypt финансировался Чалкером из собственного кармана. Он отказался раскрыть общую сумму финансирования.

Сервис Qrypt доступен для ознакомления через бесплатную учетную запись на веб-сайте, которая предлагает создать бесплатную учетную запись.

Помимо таблицы данных Qrypt на ее веб-сайте, дополнительный интересный материал можно найти в двух патентах США, выданных фирме в 2019 году. Один, «Сквозное шифрование с двойным храповым механизмом и обменом эпохальными ключами», приписывается Mandich и Додис описывает алгоритм распределения между двумя взаимодействующими устройствами асимметричной функции генерации ключей.

Второй патент, «Сеть агрегирования и распределения энтропии и случайности из нескольких источников», описывает сеть как услугу для распределения энтропии». ***(Tiernan Ray. Qrypt's cloud service will distribute entropy for better cryptography // ZDNet (https://www.zdnet.com/article/qrypts-cloud-service-will-distribute-randomness-for-better-crypto/). 09.06.2021).***

***

**«Ученые создали технологию кибербезопасности под названием Shadow Figment, которая предназначена для того, чтобы заманить хакеров в искусственный мир, а затем остановить их от нанесения ущерба, скармливая им иллюзорные лакомые кусочки успеха.**

Цель состоит в том, чтобы изолировать плохих актеров, увлекая их привлекательным, но вымышленным миром.

Технология нацелена на защиту физических объектов – инфраструктуры, такой как здания, электросети, системы водоснабжения и канализации и даже трубопроводы. Технология была разработана учеными Тихоокеанской северо-западной национальной лаборатории Министерства энергетики США.

Отправной точкой для Shadow Figment является часто применяемая технология, называемая приманкой – что-то привлекательное, чтобы заманить злоумышленника, возможно, желанная цель с видимостью легкого доступа.

Но в то время как большинство приманок используются для заманивания злоумышленников и изучения их методов, Shadow Figment идет гораздо дальше. Технология использует искусственный интеллект для развертывания изощренного обмана, чтобы удерживать злоумышленников в воображаемом мире – вымысле – который отражает реальный мир. Приманка взаимодействует с пользователями в режиме реального времени, реалистично реагируя на команды.

«Наше намерение состоит в том, чтобы взаимодействие выглядело реалистичным, чтобы, если кто-то взаимодействует с нашей приманкой, мы поддерживаем его участие, давая нашим защитникам дополнительное время для ответа», – сказал Томас Эдгар, исследователь кибербезопасности PNNL, руководивший разработкой Shadow Figment.

*Использование «успеха» злоумышленников*

Система вознаграждает хакеров ложными сигналами об успехе, удерживая их занятыми, пока защитники узнают о методах злоумышленников и предпринимают действия для защиты реальной системы.

Достоверность обмана зависит от программы машинного обучения, которая учится, наблюдая за реальной системой, в которой она установлена. Программа реагирует на атаку, посылая сигналы, которые демонстрируют, что атакованная система отвечает правдоподобным образом. Этот «управляемый моделями динамический обман» намного более реалистичен, чем статическая ловушка, более распространенный инструмент, который быстро распознается опытными кибератаками.

Shadow Figment охватывает два мира, которые несколько лет назад были независимыми, но теперь взаимосвязаны: кибер-мир и физический мир со сложными структурами, которые полагаются на сложные системы промышленного управления. Такие системы чаще, чем когда-либо, оказываются под прицелом хакеров. Примеры включают демонтаж значительной части электросети на Украине в 2015 году, нападение на систему водоснабжения Флориды в начале этого года и недавний взлом колониального трубопровода, который повлиял на поставки бензина на восточном побережье.

Физические системы настолько сложны и огромны, что количество потенциальных целей – клапаны, элементы управления, насосы, датчики, охладители и т.д. – безгранично. Тысячи устройств работают вместе, чтобы обеспечить нам бесперебойное электроснабжение, чистую воду и комфортные условия труда. Злонамеренно введенные в систему ложные показания могут привести к отключению электричества. Они могут поднять температуру в здании до неудобного или небезопасного уровня или изменить концентрацию химикатов, добавляемых в воду.

Shadow Figment создает интерактивные клоны такой системы во всей их сложности способами, которые ожидают опытные операторы и киберпреступники. Например, если хакер выключает вентилятор в серверной комнате в искусственном мире, Shadow Figment в ответ сигнализирует, что движение воздуха замедлилось и температура повышается. Если хакер изменяет настройку водогрейного котла, система соответствующим образом регулирует расход воды.

*Shadow Figment: подрыв злых умыслов*

Цель состоит в том, чтобы отвлечь злоумышленников от реальных систем управления, направить их в искусственную систему, где их действия не имеют никакого влияния.

«Мы тянем время, чтобы защитники могли принять меры, чтобы предотвратить плохие вещи», – сказал Эдгар. «Иногда даже несколько минут – это все, что вам нужно, чтобы остановить атаку. Но Shadow Figment должен быть частью более широкой программы защиты от кибербезопасности. Нет единственного решения, которое было бы волшебной пулей».

PNNL подала заявку на патент на технологию, лицензию на которую получила компания Attivo Networks. Shadow Figment – одна из пяти технологий кибербезопасности, созданных PNNL и объединенных в пакет под названием PACiFiC…

Последние результаты команды были опубликованы в весеннем выпуске Journal of Information Warfare.

Среди коллег Эдгара по проекту – Уильям Хофер, Хуан Брэнди-Лозано, Гарретт Сеппала, Кэти Новак и Драгуна Враби. Работа финансировалась PNNL и Управлением технологических переходов Министерства энергетики США». ***(PNNL's Shadow Figment Technology Foils Cyberattacks // Newswise, Inc (https://www.newswise.com/doescience/pnnl-s-shadow-figment-technology-foils-cyberattacks/?article_id=752248). 02.06.2021).***

***

**«Исследователи из Университета Рочестера создали TimeCache, подход к безопасности системы, который, как утверждается, защищает от атак по побочным каналам, таких как evict + reload и Spectre, без обычного вредного воздействия на производительность.**

2018 год не был удачным для производителей микросхем или их пользователей, когда был обнародован ряд новых атак, направленных против самих изменений дизайна, внесенных для повышения производительности на протяжении многих лет. Известные как Meltdown и Spectre, уязвимости существуют в самих

процессорах и позволяют процессам либо получать доступ, либо делать выводы о содержимом памяти, используемой другими процессами, получая доступ ко всему, от паролей до криптографических ключей.

Хотя сами недостатки связаны с аппаратным обеспечением, исправления появились в микрокоде и программном обеспечении. К сожалению, но неудивительно, учитывая уязвимость оборудования, предназначенного для повышения производительности, это означает, что они могут замедлять определенные рабочие нагрузки. Даже после исправлений все время обнаруживаются новые уязвимости, используемые атаками по побочным каналам, в том числе атака с подтверждением концепции, выпущенная Google еще в марте этого года.

Создатели TimeCache – Дивья Оджа и Сандхья Двааркадас из факультета компьютерных наук Университета Рочестера – утверждают, что это может быть ответом. Нацеленная на конкретный подкласс атак по побочным каналам против кеша, осуществляемого совместно используемым программным обеспечением, TimeCache, как утверждается, предлагает идеальную защиту с незначительным влиянием на производительность, сохраняя при этом в первую очередь все прекрасные преимущества совместного использования вещей.

*Производительность и защита наконец-то вместе*

«Наша защита от побочных каналов синхронизации с помощью общего программного обеспечения сохраняет преимущества, позволяющие процессам использовать всю емкость общего кэша», – пояснили они в документе, представленном на 48-м ежегодном международном симпозиуме ACM / IEEE по компьютерной архитектуре (ISCA). «[Это] позволяет снизить нагрузку на кэш и память за счет дедупликации данных и совместного использования копирования при записи».

Основная концепция TimeCache заключается в том, что он включает в себя информацию о предыдущем доступе к строке кэша, поэтому первый доступ данного процесса к кешу откладывается. Это означает, что невозможно сделать вывод, запросил ли другой процесс, работающий в той же системе, те же данные первым.

«Мы достигаем своей цели, – пояснили исследователи, – реализуя видимость строки кэша для каждого процесса, чтобы процессы не получали выгоды от кэшированных данных, внесенных другим процессом, пока они не понесли соответствующие штрафы за промах». Решение работает на всех уровни кэша без необходимости ограничивать количество доменов безопасности и защищает от атакующего процесса, работающего на том же ядре, в другом гиперпотоке или на другом ядре».

*Требуются модификации оборудования*

Конечно, есть загвоздка. TimeCache не может быть реализован чисто программно и требует модификации оборудования с добавлением отдельной строки кэша, каждого бита безопасности аппаратного контекста, получившего название «s-бит»; метка времени для каждой строки кэша; регистр сдвига; и логический блок последовательного побитового сравнения временных меток и параллельных логических устройств с транспонированным вентилем и

периферийными устройствами битовой линии для ускорения сравнения временных меток.

Эти модификации добавляют свои собственные накладные расходы, которые могут ощущаться в той самой среде, где безопасность общего программного обеспечения представляет наибольший интерес: в центре обработки данных.

«Общее количество s-битов [требуется] может быть значительным для LLC [Last Level Cache] в процессорах серверного класса», – признала команда, указывая на методы, уже используемые для масштабирования каталогов согласованности, которые можно применить к TimeCache, чтобы уменьшить накладные расходы на область до O (log (n)) вместо n бит на строку кэша».

Чтобы подтвердить эту концепцию, исследователи протестировали TimeCache с помощью симулятора архитектуры gem5. Система доказала свою способность защищаться от явной утечки информации в тесте микробенчмарка, активной атаке на версию GnuPG алгоритма безопасности RSA с использованием атаки flush + reload, которая работала как на реальном оборудовании, так и в моделировании без TimeCache, но была заблокирован, когда он был реализован. Это продемонстрировало, что его реализация не добавляла никаких дополнительных побочных каналов, которые можно было бы использовать.

Влияние на производительность было незначительным. Тестирование с помощью тестов SPEC2006 и PARSEC показало, что средняя накладная нагрузка составляет всего 1,13% – небольшое влияние на то, что кажется всеобъемлющей защитой от целого класса атак.

*Получение TimeCache для пользователей*

Подход TimeCache может в конечном итоге появиться в бесплатных архитектурах с открытым исходным кодом до того, как кто-либо, использующий проприетарные микросхемы, поймет.

«Чтобы полностью оценить изменения конструкции ЦП, исследователям необходим доступ к средам моделирования на разных уровнях абстракции, а также к полным источникам RTL», – заявил Стефан Валлентовиц, профессор Мюнхенского университета прикладных наук и директор RISC-V и некоммерческой организации. Фонд FOSSi, посвященный созданию сообщества и экосистемы вокруг бесплатного кремния с открытым исходным кодом, в ответ на этот документ.

«В отличие от проприетарных альтернатив, бесплатные микросхемы с открытым исходным кодом и экосистема RISC-V предоставляют сегодня многие из этих компонентов, позволяя исследователям оценивать свои идеи на всех уровнях абстракции и даже делиться своими реализациями, чтобы другие могли воспроизводить и развивать,» – добавил он.

«С точки зрения разработчиков приложений, защищающих от уязвимостей в стиле Spectre, лучший подход – абстрагироваться от защиты от разработчиков», – высказал мнение эксперт по безопасности приложений Шон Райт о потенциальном влиянии технологии TimeCache. «Под этим я подразумеваю встраивание защиты в структуру, операционную систему или наличие простых в использовании библиотек».

Он продолжил: «Разработчики часто вынуждены предоставлять новые функции, и у них нет времени на попытки реализовать какую-либо форму механизма защиты безопасности, не говоря уже о наличии достаточных знаний для этого».

Дополнительные сведения о TimeCache, который можно использовать вместе с другими средствами защиты, включая рандомизацию кеша, можно найти в этой копии документа в формате PDF: «TimeCache: использование времени для устранения боковых каналов кеша при совместном использовании программного обеспечения». ***(Gareth Halfacree. TimeCache aims to block side-channel cache attacks – without hurting performance // The Register (https://www.theregister.com/2021/06/15/timecache_aims_to_block_sidechannel/). 15.06.2021).***

***

**«Google предложила структуру, называемую SLSA, для борьбы с атаками на цепочку поставок, угрозой безопасности, примером которой является недавняя компрометация платформы мониторинга ИТ SolarWinds Orion.**

SLSA – сокращение от «Уровни цепочки поставок для программных артефактов» и произносится как «сальса» для тех, кто склонен добавлять удобные гласные – стремится обеспечить руководство по безопасности и программную гарантию, чтобы помочь защитить процесс сборки и развертывания программного обеспечения.

«Цель SLSA – улучшить состояние отрасли, особенно с открытым исходным кодом, для защиты от наиболее серьезных угроз целостности», – заявили в своем блоге в среду Ким Левандовски, менеджер по продукту Google, и Марк Лодато, инженер-программист Google. «С SLSA потребители могут делать осознанный выбор в отношении уровня безопасности программного обеспечения, которое они используют».

В последнее время участились атаки на цепочки поставок, пытающиеся использовать слабые места в конвейере создания и распространения программного обеспечения. Помимо инцидента с SolarWinds и эксплуатации уязвимостей в Apache Struts, было совершено множество атак на реестры программных пакетов, такие как npm, PyPI, RubyGems и Maven Central, на которые разработчики библиотек внутреннего кода полагаются для поддержки сложных приложений.

Согласно данным компании по обеспечению безопасности Sonatype [PDF], количество атак на проекты с открытым исходным кодом увеличилось на 430% в течение 2020 года. Одна из возможных причин заключается в том, что компрометация зависимости в широко используемой библиотеке обеспечивает широкое распространение вредоносных программ. Как отмечается в исследовательском документе TU Darmstadt за 2019 год, пять лучших пакетов npm в 2018 году «охватывают от 134 774 до 166086 других пакетов, что делает их чрезвычайно привлекательной целью для злоумышленников».

*Есть собственный корм для собак*

SLSA основан на собственном процессе внутренней безопасности Google, «авторизация двоичных файлов для Borg», который используется рекламным гигантом более восьми лет и в настоящее время является обязательным для любой производственной нагрузки. Он состоит из стандартов (правил), аккредитации (с помощью которой может быть установлено соответствие стандартам) и технических средств контроля (подписанные метаданные для автоматизированных структур политик).

В настоящее время SLSA – это более или менее полезный совет по безопасности. Но есть надежда, что это станет чем-то большим.

«В своей окончательной форме SLSA будет отличаться от списка передовых практик своей возможностью принудительного исполнения: он будет поддерживать автоматическое создание проверяемых метаданных, которые могут быть введены в механизмы политик для предоставления «сертификации SLSA» конкретному пакету или платформе сборки», объясните Левандовски и Лодато.

Предусмотрены четыре уровня соответствия. Самый высокий, SLSA 4, включает в себя два человека, просматривающих все изменения, и герметичный, воспроизводимый процесс сборки как способ убедиться, что ничего не было изменено.

Есть надежда, что SLSA поможет выявить такие проблемы, как лицемерные коммиты, скомпрометированные платформы управления версиями, злонамеренно измененная или скомпрометированная инфраструктура сборки, искаженные зависимости, опасные артефакты сборки, захваченные репозитории и атаки типа сквоттинга.

По поводу безопасности Google и ISRG, некоммерческая организация Let's Encrypt и других полезных проектов, заявили в четверг, что с апреля они финансируют разработчика Мигеля Охеда для работы над Rust для Linux и других проектов безопасности и планируют сделать так в течение года. Ожидается, что добавление большего количества кода Rust в ядро Linux уменьшит количество ошибок безопасности памяти.

«Поскольку [ядро Linux] написано в основном на языке C, который не является безопасным для памяти, уязвимости безопасности памяти, такие как переполнение буфера и использование после освобождения, являются постоянной проблемой», – пояснил Джош Аас, исполнительный директор ISRG, в сообщение в блоге.

«Сделав возможным писать части ядра Linux на Rust, который является безопасным для памяти, мы можем полностью устранить уязвимости безопасности памяти в некоторых компонентах, таких как драйверы». ***(Thomas Claburn. Google dishes out homemade SLSA, a recipe to thwart software supply-chain attacks // The Register (https://www.theregister.com/2021/06/18/google_slsa_supply_chain_rust/). 18.06.2021).***

***

**«Новая возможность Microsoft Defender для Endpoint по отслеживанию и защите неуправляемых устройств теперь стала общедоступной.**

Microsoft Defender для конечных точек (ранее Defender ATP) предоставляет группам безопасности видимость неуправляемых устройств, работающих в их сетях. Это облачная служба безопасности, которая предоставляет группам безопасности инструменты для реагирования на инциденты и расследования инцидентов и работает как экземпляр в Azure. Он отличается от антивируса Microsoft Defender, который поставляется с Windows 10.

Как сообщал в то время ZDNet, Microsoft разместила общедоступную предварительную версию этой возможности неуправляемого устройства в апреле. Эта функция направлена на снижение постпандемических рисков безопасности гибридной работы, когда люди могут использовать свои собственные компьютеры и устройства из дома, а затем приносить их на работу и подключаться к корпоративной сети.

Он предназначен для борьбы с неизвестными угрозами, которые могут исходить от устройств, которые были взломаны дома, а затем введены в работу.

Новые возможности должны упростить обнаружение и защиту неуправляемых ПК, мобильных устройств, серверов и сетевых устройств в бизнес-сети.

Выпуск GA позволяет группам безопасности обнаруживать устройства, подключенные к корпоративной сети, бортовые устройства после их обнаружения, а затем анализировать оценки и устранять угрозы и уязвимости на вновь обнаруженных устройствах.

Defender for Endpoint позволит командам обнаруживать неуправляемые рабочие станции, серверы и мобильные конечные точки на платформах Windows, Linux, macOS, iOS и Android, которые не были встроены и не защищены.

Он также охватывает сетевые устройства, такие как коммутаторы, маршрутизаторы, межсетевые экраны, контроллеры WLAN, шлюзы VPN. Их также можно обнаружить и внести в инвентарь устройств с помощью периодических проверок подлинности предварительно настроенных сетевых устройств.

Группы безопасности смогут увидеть новые функции для неуправляемых устройств в пользовательском интерфейсе Защитника Microsoft 365 в разделе «Инвентаризация устройств».

«Теперь, когда эти функции стали общедоступными, вы заметите, что обнаружение конечных точек уже включено в вашем клиенте. Об этом свидетельствует баннер, который отображается в разделе Endpoints \ Device inventory консоли Microsoft 365 Defender», – сказал Крис Халлум из Microsoft.

Баннер исчезнет 19 июля 2021 года, а поведение по умолчанию для обнаружения будет переключено с базового на стандартное. Стандартное обнаружение – это метод активного обнаружения, который использует уже управляемые устройства для проверки сети на наличие неуправляемых устройств.

«В настоящее время стандартное обнаружение позволит собирать более широкий спектр свойств, связанных с устройством, а также будет выполнять улучшенную классификацию устройств. Во время общедоступного предварительного просмотра было проверено, что переход в стандартный режим имеет незначительные последствия для сети», – сказал Халлум». ***(Liam Tung. Microsoft's security tool can now spot rogue devices on your network // ZDNet***

***(https://www.zdnet.com/article/microsofts-security-tool-can-now-spot-rogue-devices-on-your-network/). 24.06.2021).***

***

**«Исследователи из Школы инженерии и прикладных наук Колумбийского университета продемонстрировали два новых подхода к обеспечению компьютеров с защитой памяти без ущерба для производительности – и они реализуются на кристалле Исследовательской лабораторией ВВС США.**

Современные процессоры – это волшебство, но, как и любое волшебство, они иногда могут работать неожиданным образом. Возьмем, к примеру, семейства уязвимостей Spectre и Meltdown: фреймворки спекулятивного исполнения, добавленные для повышения производительности, превратились в благо для бездельников, стремящихся получить доступ к секретам, скрытым в предположительно защищенных областях памяти.

За годы, прошедшие с момента их раскрытия, были выпущены исправления для Spectre, Meltdown и целого ряда связанных уязвимостей. Однако для некоторых рабочих нагрузок лекарство может быть хуже, чем болезнь: отчет, выпущенный на этой неделе, показал, что определенные рабочие нагрузки работают в 1,6-2 раза медленнее, чем на той же платформе, без исправлений.

«Безопасность памяти была проблемой в течение почти 40 лет, и было предложено множество решений», – сказал Симха Сетумадхаван, доцент Колумбийского университета.

«Мы считаем, что безопасность памяти продолжает оставаться проблемой, потому что она несправедливо распределяет нагрузку между разработчиками программного обеспечения и конечными пользователями. Мы считаем, что с помощью этих двух документов мы нашли правильный баланс между нагрузками».

«No-FAT и ZeRØ – два важных шага к решению давней проблемы», – согласился Мигель Арройо, доктор философии, соавтор двух статей. «Атаки на безопасность памяти обходятся киберсообществу в миллионы долларов. Теперь мы можем избежать этого и обеспечить безопасность всех данных – это беспроигрышный вариант!»

Первый из документов, ZeRØ (вы можете посмотреть презентацию здесь), представляет новый набор инструкций памяти и новую схему кодирования метаданных, предназначенную для защиты как кода, так и указателей вычислительной системы. Требуя, как заявили его изобретатели, лишь незначительных изменений в архитектуре и простоты добавления в современные процессоры, ZeR0 обеспечивает защиту с нулевой потерей производительности – отсюда и название.

«ZeRØ предлагает бесплатную защиту памяти и является прекрасным дополнением к системам, уменьшающим атаки на память», – сказал соавтор статей, аспирант четвертого курса Мохамед Тарек. «Ключом к широкому распространению технологий безопасности являются низкие накладные расходы и удобство».

Вторая статья, No-FAT, в первую очередь направлена на сокращение накладных расходов на проверку безопасности памяти. Разработанный для значительного повышения скорости фаззингового анализа, автоматизированного подхода к поиску уязвимостей безопасности, No-FAT использует группирование памяти для повышения производительности.

В качестве дополнительного бонуса No-FAT вводит собственную защиту от определенных типов уязвимостей спекулятивного исполнения, включая исходный вариант Spectre, с очень низкой стоимостью производительности, измеряемой примерно 8% в тесте SPEC CPU2017. Более того, он может повысить производительность сборки мусора на языках, безопасных для памяти, и может предоставить платформу для повышения предсказуемости предварительной выборки из памяти и контроллеров динамической RAM (DRAM).

*Премия за идеи*

Высокие заявления исследователей, похоже, привлекли внимание военного комплекса США. Работа была частично профинансирована за счет грантов Управления военно-морских исследований и ВВС США, а также стипендии Qualcomm Innovation Fellowship и того, что университет описывает как «подарок от Bloomberg», и внедряется в дизайн процессора в ВВС Исследовательская лаборатория.

«В настоящее время программы-вымогатели поражают предприятия по всему миру и выходят из-под контроля», – сказал The Register британский эксперт ESET по кибербезопасности Джейк Мур. «Обычные методы смягчения воздействия явно не соответствуют требованиям стандартов. Поэтому любые новые идеи горячо оспариваются и с радостью принимаются.

«При постоянном потоке атак это новое исследование теоретически выглядит полезным для пресечения попыток – но настоящее доказательство находится в пудинге, и только время покажет, сможет ли оно противостоять шквалу ежедневных атак. узнали, что субъекты угроз настойчивы в своих действиях, и кругосветное плавание у них в крови».

Колумбийский университет опубликовал целевые страницы как для ZeR0, так и для No-FAT, со ссылками на скачивание препринтов статей на условиях открытого доступа». ***(Gareth Halfacree. Boffins promise protection and perfect performance with new ZeRØ, No-FAT memory safety techniques // The Register (https://www.theregister.com/2021/06/23/zero_no_fat_memory_safety/). 23.06.2021).***

***

**«Альянс FIDO Alliance, преследующий не меньшую миссию, чем «уменьшить чрезмерную зависимость мира от паролей», объявил о выпуске новых руководящих принципов взаимодействия с пользователем (UX), направленных на привлечение более технофобных к работе.**

Созданный еще в 2013 году как Fast Identity Online Alliance, альянс FIDO Alliance стремится полностью избавиться от паролей за счет внедрения совместимых со стандартами «аутентификаторов», включая защитные ключи USB, считыватели отпечатков пальцев, доверенные платформенные модули (TPM) и многое другое.

Хотя стандарты организации, которые были обновлены с запуском FIDO2 в 2018 году, получили признание в большинстве веб-браузеров и в ряде компаний, они по-прежнему считаются необычными и даже неудобными по сравнению со старым добрым именем пользователя и Комбинация паролей – вот где появляются новые рекомендации по UX.

«Хотя FIDO определенно предлагает более простой и надежный подход к аутентификации пользователей, по-прежнему существует потребность в том, чтобы пользователи более привыкли к пользовательскому опыту – и максимально оптимизировали эти потоки», – признал исполнительный директор FIDO Alliance Эндрю Шикиар.

Короче говоря, «если вы построите это, они придут» не всегда достаточно для технологий, меняющих парадигму. Мы слышали от все большего и большего числа доверяющих сторон, что им были бы полезны советы о том, как наиболее эффективно реализовать FIDO. это находит отклик у потребителей и работает в основных браузерах и платформах», – добавил он.

В ответ на это Альянс FIDO запустил целевую группу, ориентированную на взаимодействие с пользователем, которая получает информацию от пользователей FIDO, включая Facebook, Google, eBay, Microsoft, Visa и другие. Его цель состояла в том, чтобы выяснить, что отталкивает людей от принятия FIDO, и исправить это.

Итоговый набор рекомендаций сконцентрирован на одном варианте использования: вход в службы с поддержкой FIDO на рабочем столе. Альянс FIDO подтвердил, что другие варианты использования, включая использование мобильных устройств, будут рассмотрены в будущем – без указания точной даты выпуска соответствующих руководств.

«К сожалению, мы остро нуждаемся в защищенных от фишинга и повышающих конфиденциальность способах входа в систему, поскольку злоумышленники становятся лучше нацеливаться на свою жертву», – сказал The Register британский эксперт ESET по кибербезопасности Джейк Мур. «Многие скромные жертвы по-прежнему счастливы оставлять свои аккаунты незащищенными и уязвимыми, не зная, как их обезопасить».

Он продолжил: «Старинный баланс между безопасностью и удобством часто по-прежнему способствует простоте использования учетных записей многих людей, поэтому любые дополнительные усилия по устранению паролей для тех, кто нуждается в такой поддержке, всегда будут с благодарностью приняты».

В то же время, когда были опубликованы рекомендации по UX, FIDO Alliance объявил об обновлениях спецификаций FIDO2, направленных на упрощение корпоративного развертывания для входа в систему без пароля, включая добавление корпоративной аттестации, поддержку iFrames из разных источников и совместимость со службой аттестации Apple Attest.

«Конечная цель FIDO Alliance – как можно скорее увидеть, как как можно больше поставщиков услуг откажутся от аутентификации на основе пароля», – заключил Шикиар. «Мы надеемся, что эти руководящие принципы UX помогут ускорить это движение». ***(Gareth Halfacree. Would-be password-killer FIDO Alliance aims to boost uptake with new UX guidelines // The Register***

***(https://www.theregister.com/2021/06/24/wouldbe_passwordkiller_fido_alliance_aims/) . 24.06.2021).***

***

**«В июне 2021 года российская компания StormWall начала работать на рынке США.** Это шестьдесят восьмое иностранное государство, где компания начала оказывать услуги по защите онлайн-ресурсов от DDoS-атак. Теперь любая организация США может использовать профессиональные решения защиты StormWall. За счет расширения международной экспансии компания планирует вдвое увеличить объем бизнеса.

Согласно аналитическому отчету Mordor Intelligence, на США приходится 30% всех DDoS-атак в мире, что объясняет востребованность профессиональных решений защиты на американском рынке. Кроме того, количество DDoS-атак в США быстро растет, в настоящее время число атак достигло рекордно высокого уровня, в первую очередь, благодаря быстрому увеличению числа подключенных устройств в регионе. StormWall предложит американским компаниям целый спектр высокотехнологичных продуктов, обеспечивающих надежную защиту онлайн-сервисов от DDoS-атак любой сложности. В первые месяцы работы StormWall в США планирует продвигать свои ключевые решения: защиту сайтов, защиту сети с подключением по протоколу BGP и защиту сервисов TCP/UDP. Помимо этого, представители бизнеса смогут получить круглосуточную техническую поддержку и консультации специалистов по использованию решений StormWall.

StormWall планирует поддерживать интерес бизнеса к профессиональным решениям защиты. Для новых клиентов в США компания StormWall предложила программу лояльности, позволяющую бесплатно подключить решения защиты в тестовом режиме на 10 дней, чтобы оценить возможности продуктов. В рамках триального периода можно будет воспользоваться полной функциональностью решений.

«Мы высоко оцениваем спрос на услуги защиты от DDoS-атак на рынке США и считаем, что у нас отличные перспективы развития бизнеса на американском рынке. США всегда были и остаются самой атакуемой страной в мире. Кроме того, в последнее время значительно увеличилось количество кибератак на американские компании. Все больше организаций стремятся подключить профессиональную защиту от DDoS-атак, чтобы обезопасить свои ресурсы. Стабильный спрос на профессиональные решения защиты среди американских компаний стал уверенным трендом рынка. Мы искренне надеемся, что выход StormWall на рынок США поможет бизнесу успешно развиваться и процветать», – отметил Рамиль Хантимиров, CEO и сооснователь StormWall». ***(Владимир Бахур. Разработчик решений защиты от DDoS-атак StormWall выходит на рынок США // CNews (https://www.cnews.ru/news/line/2021-06-29_razrabotchik_reshenij_zashchity). 29.06.2021).***

***