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

КІБЕРБЕЗПЕКА В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Інформаційно-аналітичний дайджест

№ 3 (березень)

Київ – 2021

Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест / відп. ред. О.Довгань; упоряд. О.Довгань, Л.Литвинова, С.Дорогих; Науково-дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В.І.Вернадського. – К., 2021.– №3 (березень) . – 253с.

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

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

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

ЗМІСТ

«Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України попереджає про активну експлуатацію вразливостей у поширеному програмному продукті Microsoft Exchange.

…про це повідомляє РНБО.

“У разі успішної експлуатації вразливостей атакуючі мають можливість виконати довільний код у вразливих системах та отримати повний доступ до скомпрометованого сервера, включно із доступом до файлів, електронної пошти, облікових записів тощо. Крім того, успішна експлуатація вразливостей дозволяє отримати несанкціонований доступ до ресурсів внутрішньої мережі організації”, - ідеться у повідомленні.

Вразливими є локальні версії Microsoft Exchange Server 2010, Microsoft Exchange Server 2013, Microsoft Exchange Server 2016, Microsoft Exchange Server 2019. Інформація щодо вразливостей у хмарних версіях Microsoft 365, Exchange Online, Azure Cloud відсутня.

Нині активно експлуатуються вразливості CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065 (спільна назва – ProxyLogon), для вразливостей CVE-2021-26412, CVE-2021-26854, CVE-2021-27078 відсутні публічно доступні експлойти.

Найбільшу активність в експлуатації вразливих систем виявило китайське кібершпигунське угруповання Hafnium, проте нині вже підтверджено активність інших хакерських груп, з-поміж яких Tick (Bronze Butler), LuckyMouse (APT27), Calypso, Websiic, Winnti Group (BARIUM, APT41), Tonto Team (CactusPete), ShadowPad, Mikroceen, DLTMiner.

Вразливість експлуатується не лише групами, за якими стоять спецслужби, а й кіберзлочинцями. Підтверджено факти інфікування вразливих систем програмами-вимагачами, зокрема нових сімейств DearCry, DoejoCrypt. Сума викупу, яку вимагали злочинці в одному із підтверджених випадків, становила понад 16 тисяч доларів.

Скомпрометовані сервери також використовуються для розсилок шкідливого програмного забезпечення для подальшого інфікування максимальної кількості організацій. В Україні вже зафіксовано кілька таких інцидентів.

“Зазвичай після компрометації наступними фазами є розвідка (збір даних про інформаційні системи), а згодом – викрадення інформації. Це потребує певного часу, потім у багатьох випадках цінні дані шифруються або видаляються, і за них вимагають викуп. Такий механізм розвитку кібератак створює суттєві загрози втрати даних у скомпрометованих організаціях найближчим часом – від тижнів до місяців”, - додають у РНБО.

Microsoft випустила пакети оновлень для вразливих версій та програмні інструменти, призначені для самостійної перевірки наявності вразливості (https://github.com/microsoft/CSS-Exchange/tree/main/Security). За результатами аналізу установок оновлень та повідомленнями партнерів, процедура оновлення не завжди автоматично дозволяє забезпечити захист від вразливостей для усіх

мінорних версій Microsoft Exchange Server. Так, за повідомленням парламенту Норвегії, їх інформаційні системи було зламано та викрадено дані, хоча оновлення були встановлені.

Тому під час установки пакетів оновлень необхідно врахувати таке:

Оновлення необхідно застосувати з командного рядка від імені користувача з правами адміністратора, після установки необхідно перезавантажити сервер.

Після завершення процесу оновлень необхідно здійснити повторну перевірку можливості експлуатації вразливості (інструменти – утиліта MSERT https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download або скрипт nmap https://github.com/GossiTheDog/scanning/blob/main/http-vuln-exchange.nse).

Раніше компанія Microsoft повідомляла про несанкціонований доступ до фрагментів вихідного коду її продуктів під час масштабної кібератаки на державні установи та приватні організації США, яка отримала назву Solorigate. Є дані, що деякі з виявлених вразливостей експлуатувалися (як вразливості нульового дня) щонайменше за 2 місяці до випуску пакетів оновлень до Microsoft Exchange Server.

Тому НКЦК рекомендує розглядати системи вразливих версій Microsoft Exchange Server та мережі, в яких вони використовуються, як скомпрометовані, та задіяти процедури реагування на інцидент. Якщо під час реагування факт компрометації не підтверджується, рекомендується посилити заходи моніторингу подій безпеки і слідкувати за розвитком ситуації, оскільки надходять нові дані про тактику, техніки та процедури дій атакуючих, та оновлюються індикатори компрометації.

Станом на 12 березня в Україні виявлено понад 1000 вразливих серверів Microsoft Exchange Server, з них 98,7% використовуються у приватному секторі.

НКЦК закликає одразу повідомляти про факти компрометації або спроби експлуатації вразливостей за адресою report@ncscc.gov.ua для скоординованого реагування. Фахівці НКЦК готові надати технічну та консультативну допомогу при реагуванні, зокрема організаціям приватного сектора.

Агентство CISA (США) рекомендує здійснювати пошук ознак компрометації щонайменше з 1 січня 2021 року.

Перевірити наявність ознак компрометації можна шляхом виконання скрипту (Microsoft) Test-ProxyLogon.ps1 (https://github.com/microsoft/CSS-Exchange/tree/main/Security)

Під час експлуатації вразливостей у скомпрометовану систему встановлюється т.зв. вебшел — скрипт, призначений для віддаленого доступу та управління (адміністрування) інфікованою системою. Зазвичай вебшел використовується для викрадення облікових даних, завантаження іншого шкідливого коду (наприклад, з метою пошуку інших жертв та їх зараження), в якості командного серверу для управління іншими інфікованими системами». ***(РНБО попереджає про високий рівень кіберзагроз через вразливість Microsoft Exchange // Укрінформ (https://www.ukrinform.ua/rubric-technology/3208523-rnbo-poperedzae-pro-visokij-riven-kiberzagroz-cerez-vrazlivist-microsoft-exchange.html). 15.03.2021).***

***

«Якою буде ваша реакція, якщо вам скажуть, що кожна людина, котра має вихід у мережу Інтернет через будь-який електронний пристрій, — ходячий компромат як особистого життя, так і корпоративного? Навіть якщо ви не посадовець з реєстру РЕР, не державний службовець категорії А/Б, не друг Сноудена, і ваш пароль на акаунтах набагато складніший за qwerty1234, ви також потенційна жертва кібератаки.

Якщо ви у цьому не впевнені, ось перелік найвідоміших цифрових атак в Україні за останні роки:

Квітень 2017 року — «вірус Петя», один із наймасштабніших вірусів у нашій державі. Petya.A — шкідливе програмне забезпечення, яке було спрямоване на мережу державних підприємств, установ, банків, медіа. Цей вірус, потрапивши до системи, безповоротно знищував оригінальні файли і примусово перезавантажував комп'ютер, після чого користувачеві виводився екран з вимогою перерахувати певну грошову суму в біткоїнах на криптогаманець. Вірус розповсюджувався через популярну та широко використовувану серед бухгалтерів програму M.E.Doc. Зокрема, цій атаці було піддано такі підприємства, як аеропорт «Бориспіль», ЧАЕС, «Укртелеком», Ощадбанк, «Укрзалізниця», а також офіційний сайт Кабінету міністрів України та численні комерційні підприємства.

Березень 2019-го — фішингова розсилка на тему виборів проводилася нібито від імені Центру соціальних і маркетингових досліджень (SOCIS). Як приманка використовувалися «інформаційні матеріали» про соціально-політичну ситуацію в Україні.

Березень 2020 року — фішингові листи на тему коронавірусу, що приховували у собі шкідливе програмне забезпечення.

Жовтень 2020-го — фішингові розсилки на працівників державних установ України з метою компрометації облікових записів електронної пошти.

Січень 2021 року — відбулася масова розсилка фішингових електронних листів на державні установи України. Листи були відправлені начебто від імені адміністрації Держспецзв'язку з поштової скриньки zapros@dsszzi.gov.ua та містили вкладення зі шкідливим програмним забезпеченням.

Лютий 2021-го — хакерське втручання в нову популярну соціальну мережу Clubhouse. Хакер-«благодійник» перенаправляв аудіопотоки розмов, що велись у Clubhouse, на інший веб-сайт, щоб інші користувачі могли слухати розмови.

Узагалі метою багатьох хакерських атак є вимагання інформації або грошей з наступним їх переказуванням на криптогаманець. Масовий перехід на дистанційну роботу — це не лише вимога сьогодення і спроба вберегтися на час пандемії, а й додатковий стимул для хакерів, які тепер можуть отримати більше від кожної нової атаки. Відновлення стану і роботи пошкоджених програм, пошкодженої чи знищеної інформації — завжди складний, а іноді тривалий і часто фінансово витратний механізм.

Від приватного до публічного і навпаки: кібербезпека — це двосторонній рух, оскільки під атаку хакера може потрапити як ваш особистий акаунт, наприклад, ваші фото на Google-сервісі, так і корпоративне хмарне сховище з усією

конфіденційною інформацією чи корпоративна електронна пошта вашої компанії, яка значиться в усіх ланках публічного простору.

Так, цифрова держава має свої недоліки, незважаючи на значні переваги, і одне з цих слабких місць — це неналежна, неефективна або в деяких випадках і відсутня кібербезпека.

Взагалі, якщо дуже стисло, то кібербезпека є однією з видів інформаційної безпеки, основна мета якої — здійснення захисту державних, персональних, корпоративних даних. Приватна інформація, в тому числі різноманітні бази даних, давно вже стала новою валютою, електронним знаряддям на віртуальному тіньовому ринку попиту і пропозиції. Адже при хакерській атаці несанкціонований витік інформації може завдати значних фінансових збитків компанії, державі або нашкодити особистій репутації окремої приватної особи.

Однак хакерська атака — це не завжди втручання зовні, інколи вірусної шкоди умисно або ненавмисно може завдати і співробітник компанії або ж приватна особа сама собі внаслідок ведення в оману. Саме тому виокремлюють два види хакерських атак — зовнішню і внутрішню.

Однією з найпоширеніших хакерських пасток є відправлення вірусного e-mail або повідомлення, так званий фішинговий лист. Фішинг — підроблений електронний лист (або SMS чи повідомлення у месенджері), який виходить начебто від офіційного джерела — компанії, колеги по роботі, друга. Щоб уникнути цього, не поспішайте одразу ж переходити за посиланням або відповідати, якщо стилістика тексту або формат повідомлення дещо відрізняється від звичної мови адресата. Краще спробуйте в інший спосіб зв’язатися з цією людиною та уточнити, чи дійсно вона відправила вам електронного листа. Те саме стосується і SMS-повідомлень, чатів у месенджерах, соціальних мережах тощо.

До речі, при крадіжці вашого смартфону, планшета тощо невідкладно почистіть акаунти та, звісно ж, попередьте всіх, з ким ви маєте тісні та важливі контакти. Оскільки не секрет, що майже всі месенджери дозволяють видалити інформацію в чатах у двосторонньому напрямку.

Для компаній, як державних, так і приватних, що, крім корпоративної електронної пошти, мають внутрішні робочі програми, сервісні сховища, краще не економити на штатному спеціалісті по захисту систем електронної інформації або ж мати таку нештатну довірену особу.

Якщо все ж таки на вашому підприємстві стався критичний витік інформації або відбулося глобальне несанкціоноване втручання в програмні пристрої, електрону базу даних, крім невідкладних технічних та етичних дій з попередження поширення інформації надалі, спершу необхідно провести внутрішнє розслідування, аби виключити варіант хакерської умисної атаки зсередини компанії серед ваших співробітників.

Для здійснення такого внутрішнього розслідування скликається комісія з представників органів управління, керівників відділів, представників профспілки (якщо такий орган передбачений), внутрішнього або залученого юриста, також до розслідування долучається корпоративний спеціаліст із захисту систем електронної інформації. За можливості скористайтеся послугами незалежного форензік-спеціаліста або експерта з розслідування кіберзлочинів.

До речі, якщо в вашій компанії працює спеціаліст із захисту електронної інформації на договірній (за трудовим законодавством) або контрактній основі, притягнути його до відповідальності або до матеріального відшкодування спричинених компанії збитків без належного внутрішнього розслідування, в односторонньому порядку буде не так просто. Будьте готові, що справа може дійти і до суду, і саме ваша сторона має буде довести, що внаслідок халатних, непрофесійних дій або бездіяльності вашого спеціаліста виникла кібератака, внаслідок чого підприємство зазнало матеріальних збитків.

Звісно, ви також маєте право, а за деяких обставин, якщо кібератака стосується державних і/або суспільних інтересів, просто зобов'язані звернутись із заявою до спеціального відділу розслідувань поліції. На щастя, в останні роки українська влада значно збільшила увагу до цього питання.

В Україні основним законодавчим регулюванням питань кібербезпеки є Закон «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року, Конвенція про кіберзлочинність від 21 листопада 2001 року, ратифікована нашою країною у вересні 2005 року, а також Кримінальний кодекс України.

Відповідно до законодавства основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних сил України, розвідувальні органи, Національний банк України.

Також спеціальними робочими державними органами є: Національний координаційний центр кібербезпеки, утворений відповідно до рішення РНБО України від 27 січня 2016 року, та Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, на сайті якої ви можете онлайн повідомити про кіберзлочин та отримати належну допомогу.

З 2009 року CERT-UA є акредитованим членом Форуму команд реагування на інциденти безпеки FIRST — провідної організації та визнаним світовим лідером у цій сфері.

Питання покращення кібербезпеки в Україні за останні кілька років перейшло зі стану проміжних обговорень до вирішення актуальних проблем і реагування.

Така зацікавленість, а точніше, нагальна необхідність зумовлена діджиталізацією суспільства, розвитком і впровадженням урядом цифрової політики в сфері надання державних послуг, а також, на жаль, одним із головних чинників актуальності цієї теми — збільшенням хакерських атак, особливо підривом електронних державних програм, сервісів і баз даних.

Якщо звернемося до судової практики розгляду питань з кібербезпеки, то в Україні найпоширенішими є злочини, що підпадають під статтю 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації) та статтю 361-1 Кримінального кодексу України (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), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку).

Саме тому уряди розвинених держав за підтримки різних організацій, у тому числі міжнародних, недержавних, через державно-приватні соціальні проєкти, розробляють нові механізми кіберзахисту і працюють над ними. А саме: покращують цифрову обізнаність громадян, створюють стимулюючу систему для найкращих ІТ-кадрів, удосконалюють роботу зі створення вітчизняних програмних продуктів для захисту державних інформаційних ресурсів, зокрема національної операційної системи, національного антивірусного програмного забезпечення тощо, та періодично підвищують компетентність фахівців різних сфер діяльності з питань кібербезпеки.

Ахіллесова п'ята кібербезпеки — це стрімкий постійний розвиток електронних програм, методів дистанційного та майже невпізнаного керування. А також недоступність для більшості пересічних користувачів навичок та інструментів, які можуть убезпечити «цифрову» частину їхнього життя». ***(Дар'я Скоблікова. Гігієна в часи діджиталізації // Дзеркало тижня. Україна (https://zn.ua/ukr/tech/hihijena-v-chasi-didzhitalizatsiji.html). 18.03.2021).***

***

«Розв'язувати спільно проблему кібербезпеки школярів мають представники влади, вчителі, батьки, психологи і поліцейські.

Так вважають ініціатори унікального для України проекту "Ювенальний Поліцейський Інспектор", який у квітні стартує в семи школах краю.

Не секрет, що власні сторінки в соцмережах мають навіть шестирічки. Тому важливо навчити дітей безпечно ними користуватися.

Передбачається, що спеціально навчені ювенальні поліцейські працюватимуть у навчальних закладах Кам'янського, Криничок, Нікополя, Новомосковська, Петриківки, Покровського і Синельниківського районів.

"Усі ювенали пройшли спеціальні тренінги. Розмовлятимуть зі школярами, батьками, вчителями про те, як уберегти дитину від небезпеки в соцмережах і куди звертатися у разі кіберзагроз", - розповіла начальник відділу управління ювенальної діяльності ГУ НП в області Наталія Лазаренко.

Схильність до спілкування в соцмережах - один з видів підліткової залежності. Допомогти дитині позбутися її можуть саме батьки, наголосив керівник психологічної служби системи освіти області Віктор Мушинський: «Найефективніший метод боротьби з кібернебезпекою - не батьківський контроль, а емоційний контакт з дитиною». ***(Ігор ТЬОМІН. Дніпропетровщина: Дітей навчать кібербезпеки // Голос України (http://www.golos.com.ua/news/132849). 26.03.2021).***

***

«Національний оператор зв'язку «Укртелеком» пропонує бізнес-абонентам послугу для захисту ІТ-інфраструктури. Вона базується на технологічних рішеннях компанії Bitdefender і надається у співпраці з Softico –

офіційним представником міжнародного постачальника в Україні – за схемою SaaS (Software as a Service) на умовах абонентської передплати для юридичних осіб, користувачів оптичного інтернету від «Укртелеком бізнес».

Нова послуга не потребує додаткових витрат на закупівлю програмного забезпечення чи обладнання і дозволяє протягом доби організувати захист кінцевих точок (Endpoint Security) для компанії будь-якого масштабу. Залежно від версії продукту клієнт отримує повноцінний захист від кіберзагроз, зокрема, спаму, шкідливих програм та вірусів, шифрувальників-вимагачів, фітингу тощо.

Поєднання послуг оптичного інтернету та антивірусного захисту може бути вигідне не лише малому бізнесу, а й державним установам та великим компаніям. Додатковою перевагою є можливість захисту серверів та «хмарної» інфраструктури». ***(Бізнес-абоненти «Укртелеком» можуть захиститися від кіберзагроз за допомогою хмарного сервісу Bitdefender // Компьютерное Обозрение (https://ko.com.ua/biznes-abonenti_ukrtelekom_mozhut_zahistitisya_vid_kiberzagroz_za_dopomogoyu_hmarnogo_servisu_bitdefender_136814). 26.03.2021).***

***

«По оценкам аналитиков DX Agent в минувшем году объем украинского рынка решений информационной безопасности уменьшился на 22% и составил ориентировочно 68 млн. долл. в ценах заказчиков (для сравнения, в 2019 г. он вырос на 52% и достиг 86 млн долл.).

Как отмечается, в структуре продаж по-прежнему преобладает ПО с долей 57% (38,8 млн долл.), четверть приходится на аппаратно-программные решения (16,8 млн долл.), причем, именно их продажи упали больше всего – на 49%, а вот доля услуг выросла на два пункта – до 18% (12 млн долл.). По прогнозам, в 2021 г. рынок IT Security в Украине ожидает незначительный рост в районе 5%.

Что касается вендоров, то состав пятерки лидеров не изменился: как и год назад, это Cisco, Check Point, Fortinet, Symantec и Eset. Однако их суммарная доля упала с 56% в 2019 г. до 50% в 2020 г. Среди крупных заказчиков, как и годом ранее, лидирует «Ощадбанк» с долей 17-18%». ***(Украинский рынок систем информационной безопасности в 2020 г. сократился на 22% до 68 млн. долл. // Компьютерное Обозрение (https://ko.com.ua/ukrainskij_rynok_sistem_informacionnoj_bezopasnosti_v_2020_g_sokratilsya_na_22_do_68_mln_doll_136728). 19.03.2021).***

***

«Заступник голови цифрового комітету Ради Олександра Федієнко оцінив можливість здійснення глобальної кібератаки такого масштабу, як вірус Petya. З 2017 року в країні суттєво підвищився рівень кібербезпеки.

Повторення атаки такого масштабу на Україну навряд чи можливо, розповів Федієнко, пише «РБК-Україна».

«Такі широкосмугові атаки, як Petya, малоймовірно провести зараз. Я особисто не бачу загрози проведення такої глобальної атаки», – зазначив фахівець.

Заступник секретаря РНБО Андрій Демедюк додав, що через майже чотири роки в Україні істотно підвищився рівень кібербезпеки. Створені та ефективно працюють відповідні підрозділи в Нацбанку, Міноборони та Мінінфраструктури.

27 червня 2017 року під час масштабної хакерської атаки тисячі серверів як державних, так і приватних підприємств України були заражені вірусом Petya (він же NotPetya). Він поширювався через оновлення популярної бухгалтерської програми.

Всього за пару годин вірус зупинив роботу сайтів великих банків, енергетичних компаній, поштових сервісів, об'єктів інфраструктури та багатьох інших ресурсів. За даними Державної служби спецзв'язку та захисту інформації, ця кібератака завдала економіці збитків на близько 10 млрд доларів. Українська сторона пов'язує атаку вірусу Petya з Росією.

Раніше кіберспеціалісти Служби безпеки України заблокували масштабну кібератаку хакерського угруповання «Armageddon», підконтрольної ФСБ РФ. Куратори могли отримати доступ до секретних даних вищих органів державної влади України.

Великобританія планує посилити свій потенціал для проведення кібератак проти ймовірних противників. Британські Національні кіберсіли повинні будуть базуватися на півночі Англії.

Адміністрація президента США Джо Байдена може сформувати цільову групу для боротьби з масштабними кібератаками, «пов'язаними з Китаєм». У «Об'єднану координаційну групу» (UCG) повинні увійти ФБР, Агентство кібербезпеки і інфраструктурної безпеки (CISA) та інші». ***(Фахівці розповіли, чи слід Україні боятися нового вірусу рівня Petya // UA.NEWS (https://ua.news/ua/spetsialisty-rasskazali-sleduet-li-ukrainy-boyatsya-novogo-virusa-urovnya-petya/). 16.03.2021).***

***

«Британська компанія WizCase, що спеціалізується на кібербезпеці, заявила, що стався витік номерів телефонів, аудіозаписів голосових дзвінків і журналів дзвінків користувачів, в основному, України і Росії. Пізніше автори внесли зміни до свого матеріалу, де підкресили, що йшлося про вразливість, а компанія Ringostat заявила, що витоку даних не було.

Автор Чейз Вільямс стверджував, що було виявлено більше двох мільярдів записів загальним обсягом понад 800 гігабайт. І вразливість нібито була в базі даних сервісу відстеження телефонних дзвінків Ringostat.

У блозі наголошувалося, що злив даних пов'язаний з компанією, що спеціалізується на відстеженні дзвінків, аналітиці та розробці маркетингових інструментів для смартфонів. Основними її ринками надання послуг є Росія і Україна. Так що користувачі в цих країнах можуть бути в зоні ризику.

У WizCase стверджували, що в мережу злили нібито близько 8 мільйонів голосових записів, приблизно 13 мільйонів телефонних номерів, сотні мільйонів журналів викликів. Також хакери нібито отримали метадані, які включають інформацію про вихідні та вхідні дзвінки, час, IP-адресу одержувача дзвінка, GSM-компанії та тривалість виклику.

Чейз Вільямс пише, що витік даних нібито був доступний будь-кому, у кого була відповідна посилання. Для доступу до інформації не було необхідності в паролі і інформація не була зашифрована. А на даний момент проблема вже усунена.

ОНОВЛЕНО

До редакції порталу звернулися представники компанії, які запевняють, що інформація про "злив" не відповідає дійсності.

"Ми зв'язалися з редактором і технічним фахівцем wizcase. Вони обидва підтвердили, що витоку не було. Редактор wizcase Деніел повідомив, що немає підтвердженого факту витоку даних в мережу. Технічний фахівець Ата каже, що була вразливість, і вона була усунена дуже оперативно (a few moments after our disclosure the server was secured). За цей час завантажити 800Гб даних неможливо. Редактор Деніел підтвердив, що їх стаття не була невірно трактована ЗМІ, витоку не було і він обіцяв внести інформацію про це в їх оригінальну статтю ", - повідомляється в листі представників компанії Ringostat». ***(Дмитрий Киришин. WizCase помилково заявила про витік телефонних дзвінків // Znaj.ua (https://life.znaj.ua/370488-wizcase-zayavila-pro-vitik-telefonnih-dzvinkiv-z-ringostat-u-samomu-operatori-ce-zaperechuyut). 04.03.2021).***

***

Правове забезпечення кібербезпеки в Україні

«Государственная служба специальной связи и защиты информации Украины обнародовала для общественного обсуждения проект Стратегии кибербезопасности Украины на 2021-2025 годы. На сайте Рады национальной безопасности и обороны (РНБО) указано, что проект уже одобрила рабочая группа при Национальном координационном центре кибербезопасности Совета национальной безопасности и обороны Украины.

Целью Стратегии кибербезопасности Украины на 2021-2025 годы определено создание условий для безопасного функционирования киберпространства, его использование в интересах личности, общества, государства. Документ основывается на принципах сдерживания, киберстойкости и взаимодействия. Координатором реализации Стратегии является Национальный координационный центр кибербезопасности.

"Киберпространство вместе с другими физическими пространствами признано одним из возможных театров военных действий, поэтому способность государства защищать национальные интересы в нем рассматривается как важная составляющая кибербезопасности. Набирает силу тенденция по созданию нового рода войск - кибервойск, в задачи которых входит не только обеспечение защиты критической информационной инфраструктуры от кибератак, но и проведение превентивных наступательных операций в киберпространстве, направленных на уничтожение вычислительных сетей и информационных систем вооруженных сил противника, а также вывода из строя критически важных объектов противника путем разрушения информационных систем, которые управляют такими

объектами, - говорится в проекте Стратегии. - В то же время все более активно применяется сочетание традиционных и нетрадиционных стратегий и тактик с использованием цифровых информационных технологий. В частности, Россия активно реализует концепцию информационного противоборства, основанную на симбиозе боевых действий в киберпространстве и информационных операций, механизмы которой активно применяются в процессе гибридной войны против Украины. Страны ЕС, НАТО, ведущие международные компании и эксперты единодушно признают Российскую Федерацию и ее действия в киберпространстве главной угрозой международной кибербезопасности. Ее разведывательно-подрывная деятельность в киберпространстве является частью гибридной войны, которую она ведет против Украины. Такая деструктивная активность создает реальную угрозу совершения актов кибертерроризма и кибердиверсий относительно национальной информационной инфраструктуры".

Прогнозируется рост интенсивности межгосударственного противоборства и разведывательно-подрывной деятельности в киберпространстве, что будет проявляться прежде всего в расширении круга государств, которые будут пытаться сформировать собственную киберразведку, овладеть современными технологиями разведывательно-подрывной деятельности в киберпространстве, усилить государственный контроль за национальными сегментами сети Интернет.

Подчеркивается, что негативным признаком технологического развития, связанного с всеобъемлющим распространением цифровых технологий, расширением Интернет-среды, является критически растущий технический уровень инструментария реализации киберугроз, от чего ландшафт таких угроз охватывает все больше сфер жизнедеятельности. Кибератаки, их разновидности становятся все более интеллектуальными и опасными, создавая реальную угрозу критически важной инфраструктуре. Злоумышленники сосредотачивают усилия на поиске уязвимостей активов (систем управления) и разрабатывают для этого уникальные по своим свойствам:

- многофункциональное вредоносное программное обеспечение,
- вирусы-шифровальщики,
- ботнеты, осуществляющие распределены атаки (DDoS) на операционные сети, производственные системы, которые используют облачные сервисы, атаки на цепи поставок.

С учетом развития технологий искусственного интеллекта в ближайшие 5-10 лет масштабы и последствия таких вмешательств будут только расти.

Рабочей группой были определены концептуальные подходы к дальнейшему развитию национальной системы кибербезопасности. Основные из них опираются на:

- всеобъемлющее понимание и анализ цифровой среды, глобальных трендов кибербезопастностной среды (с одновременным учетом особенностей нашей страны), неуклонную защиту национальных интересов Украины;
- перманентностьи мер по совершенствованию законодательства в сфере кибербезопасности;
- ориентированность на экономический и социальный рост общества;

- сбалансированное обеспечение потребностей государства и прав граждан, соблюдение законности, процессуальных гарантий и средств правовой защиты;
- определение четких ролей, потребностей, обязательств при решении задач кибербезопасности разной степени сложности;
- риск-ориентированный подход к мерам обеспечения кибербезопасности и киберзащиты;
- внедрение механизмов государственно-частного партнерства в сфере кибербезопасности;
- проактивный подход, что предусматривает осуществление предупредительных мер;
- обеспечение демократического гражданского контроля за функционированием национальной системы кибербезопасности.

Предполагается, что в первый год действия Стратегии будут безотлагательно разработаны индикаторы оценки состояния кибербезопасности и киберзащиты; проведен обзор состояния киберзащиты критической информационной инфраструктуры, государственных информационных ресурсов и информации, требование относительно защиты которой установлено законом; разработаны и внедрены механизмы проведения осмотров состояния национальной системы кибербезопасности. Это позволит при необходимости с учетом изменений в среде безопасности вносить изменения в общий план и ежегодных планов мероприятий по реализации Стратегии.

Национальный координационный центр кибербезопасности будет ежегодно обнародовать публичный отчет о реализации Стратегии и систематически информировать о решениях, событиях и ситуации в сфере кибербезопасности». ***(Герман Богапов. Украина разрабатывает Стратегию кибербезопасности на 2021-2025 годы // Internetua (http://internetua.com/ukraina-razrabatyvaet-strategiua-kiberbezopasnosti-na-2021-2025-gody). 17.03.2021).***

***

Кібервійна проти України

«У складі спецслужб РФ діють підрозділи, які ведуть підривну інформаційну війну в Україні: лише за минулий рік СБУ ліквідувала 2,5 тис. спільнот у соцмережах з мільйонною аудиторією та понад 20 ботоферм з потужністю понад 60 тис. акаунтів, які координувалися з Росії.

Про це заявив співробітник департаменту кібербезпеки СБУ Ілля Вітюк під час виступу на всеукраїнському форумі «Україна 30. Культура. Медіа. Туризм», повідомляє кореспондент Укрінформу.

«У складі спецслужб Російської Федерації, як, до речі, і в складі багатьох інших спецслужб іноземних держав, діють спеціальні підрозділи, безпосередньо функціональним завданням яких є створення сталих позицій впливу в інформаційному просторі, проведення інформаційних операцій, спеціальних інформаційних акцій, в тому числі підривних та деструктивних. Більше того, є визначені підрозділи, спеціалізація яких конкретно – Україна. Тобто це їхня робота,

люди отримують за це заробітну плату, люди отримують відповідне фінансування, відповідні інші засоби – це можуть бути державні та формально недержавні інформаційні та медіаресурси. За цю роботу вони відповідають та звітують», – повідомив Вітюк.

Він також відзначив, що в умовах гібридної війни інформаційна агресія, що організовується та координується вказаними російськими підрозділами, зростає в рази. Ці підрозділи відомі Службі безпеки України, регулярно отримуються дані, що підтверджують їхню підривну діяльність та які лягають в матеріали контррозвідувальної діяльності та кримінальних проваджень.

«Ми відмічаємо на сьогодні, що весь інформаційний простір України стає плацдармом, а інструментами стають телеканали, інформаційні портали, вебресурси, поштові сервіси, Телеграм-канали, так звані фабрики тролів, блогери, спільноти в соцмережах та ін. СБУ чітко розуміє ту межу, після перетину якої необхідно рішуче діяти, і для нас комплексний захист інформаційної безпеки – це повсякденна системна робота», – запевнив Вітюк.

За інформацією Департаменту кібербезпеки СБУ, протягом 2020 року правоохоронці викрили та заблокували діяльність більше тисяч ворожих спільнот та акаунтів.

«Лише за 2020 рік нами заблоковано понад 2,5 тис. спільнот у соціальних мережах з мільйонною аудиторією, нами заблоковано діяльність понад 20 ботоферм з потужністю більш ніж 60 тис. акаунтів, нами нейтралізовано понад 600 кібератак та кіберінцидентів на інформаційні ресурси органів державної влади, припинено діяльність 20 угруповань, причетних до таких атак, і стосовно певних з них отримана конкретна доказова база, що свідчить про те, що їхня діяльність координувалась саме з Російської Федерації. Оголошено про підозри певним блогерам та організаторам Телеграм-каналів за статтею 111 «Державна зрада» та ст.161 «Порушення рівноправності громадян», – повідомив Вітюк.

Представник СБУ розповів, що Російська Федерація ставить за мету охопити максимальну аудиторію в Україні, іноді використовуючи для впливу законні методи. Зокрема, на певних порталах роздмухується тема невдоволення владою, державними інститутами влади, що притаманне будь-якому суспільству у світі, однак є більш екстремістські напрями, коли порушуються питання суперечностей між Заходом та Сходом, що Крим – це начебто не Україна, що необхідно «зносити владу» тощо.

Вітюк запевнив, що СБУ конкретно знає, хто розкручує ці канали та яким чином вони координуються.

Він також окреслив проблеми, які на сьогодні потребують врегулювання. Зокрема, йдеться про відсутність механізму блокування ворожих медіаресурсів, проблеми із взаємодією зі світовими ІТ-гігантами, які часом відмовляються співпрацювати з Україною та ін.

Водночас Вітюк запевнив, що співпраця з РНБО дозволяє поступово викорінювати шкідливі інформаційні ресурси, та анонсував наступні кроки спецслужб.

«Найближчим часом будуть більш вагомі, більш помітні результати в боротьбі з негативною злоякісною пропагандою, не зачіпаючи при цьому здорову

інформаційну та, зокрема, журналістську спільноту», - пообіцяв посадовець…». ***(СБУ торік заблокувала в соцмережах тисячі спільнот і ботоферм, які працювали на Росію // Укрінформ (https://www.ukrinform.ua/rubric-society/3204693-sbu-torik-zablokuvala-v-socmerezah-tisaci-spilnot-i-botoferm-aki-pracuvali-na-rosiu.html). 09.03.2021).***

***

«Служба безпеки України повідомила, що її фахівці заблокували масштабну кібератаку підконтрольного ФСБ РФ хакерського угруповання «Armageddon». Через дії хакерів куратори з країни-агресора могли отримати доступ до секретних даних вищих органів державної влади України.

Як зазначається, завдяки оперативному реагуванню СБУ вдалося нейтралізувати наслідки та усунути передумови для потенційного несанкціонованого доступу російських спецслужб до державних інформаційних ресурсів.

Про виявлені кіберзагрози СБУ поінформувала органи державної влади через платформу «MISP-UA».

На цій платформі Ситуаційний центр кібербезпеки СБУ розмістив:

відповідні індикатори кіберзагроз;

рекомендації щодо заходів із виявлення і попередження фактів несанкціонованого втручання;

інструменти для пошуку шкідливого програмного забезпечення.

СБ України провела широкомасштабні заходи для локалізації кібератаки спецслужб РФ спільно з Національним координаційним центром кібербезпеки при РНБО та у взаємодії з центральними органами виконавчої влади.

Як повідомляється СБ України продовжує роботу з виявлення, фіксації і нейтралізації будь-яких проявів гібридної агресії РФ проти України, а також докладає всі зусилля для їх попередження». ***(СБУ заблокувала масштабну хакерську атаку на урядові ресурси України // Компьютерное Обозрение (https://ko.com.ua/sbu_zablokuvala_masshtabnu_hakersku_ataku_na_uryadovi_resursi_ukrayini_136682). 16.03.2021).***

***

«Росія відповіла на санкції щодо народних депутатів Віктора Медведчука і Тараса Козака («Опозиційна платформа-За життя») масштабними кібератаками на українські сайти і системи документообігу державних органів, розповів «РБК-Україна» заступник секретаря РНБО Сергій Демедюк.

Із середини лютого Національний координаційний центр кібербезпеки при РНБО фіксував як звичайні DDoS-атаки з метою «покласти» сайти потоком однотипних запитів, так і спроби заразити вірусами програми документообігу. Українській стороні вдалося вчасно виявити загрози і запобігти серйозним наслідкам.

Демедюк уточнив, що причиною атак став не лише удар по активах проросійських депутатів, а й блокування їхніх телеканалів «112 Україна», NewsOne і Zik, що використовувалися для ретрансляції пропаганди Кремля в Україні.

«Початок низки атак відбувався наче «за годинником», деякі з них виконували роль операції прикриття, щоб відвернути увагу команди реагування», - каже заступник секретаря РНБО.

За його словами, така тактика свідчить про координацію дій під час кібератак і є додатковим підтвердженням участі російських спецслужб.

Водночас росіяни активно сканують український сегмент інтернету в пошуках уразливих місць, а виявивши - запускають шкідливі програми для втручання в роботу систем і мереж.

Раніше в Службі безпеки України розповіли, що в російських спецслужбах є окремі підрозділи, які працюють виключно на розхитування ситуації у нашій країні.

2 лютого президент Володимир Зеленський своїм указом ввів у дію рішення РНБО про накладення п'ятирічних санкцій на телеканали ZiK, NewsOne, «112 Україна» та їх формального власника – члена парламентської фракції ОПЗЖ Тараса Козака. Під санкціями також опинилися літаки Козака і Віктора Медведчука, на які вони регулярно літали в Москву в обхід заборони на пряме авіасполучення з РФ. Санкції передбачають блокування активів, економічної і фінансової діяльності, анулювання ліцензій.

19 лютого РНБО ввела санкції проти 19 компаній, п'яти росіян і трьох громадян України: Віктора Медведчука і його дружини Оксани Марченко, а також Наталії Лавренюк – фактичної дружини Тараса Козака. Підставою для санкцій проти Марченко і Лавренюк стало те, що їм належить нафтопереробний завод у РФ, що постачає продукцію терористичним угрупованням «ДНР» і «ЛНР».

РНБО також ініціювала повернення державі ділянки газопроводу «Самара - Західний напрямок», який у 2017 році перейшов у власність Медведчука». ***(У РНБО розповіли про «кібервідповідь» Росії на санкції проти Медведчука та Козака // Дзеркало тижня. Україна (https://zn.ua/ukr/POLITICS/v-rnbo-rozpovili-pro-kiberotvete-rosiji-na-sanktsiji-proti-medvedchuka-i-kozaka.html). 16.03.2021).***

***

«Національний координаційний центр кібербезпеки попередив про високий рівень кіберзагроз в Україні. Це пов’язано зі вразливістю програмного забезпечення для серверів Microsoft Exchange Server.

Як повідомляє Рада нацбезпеки і оборони України (РНБО), станом на 12 березня в Україні виявили понад тисячу вразливих серверів Microsoft Exchange, майже 99% з них використовуються у приватному секторі. Такі сервери рекомендують розглядати як скомпрометовані та задіяти процедури реагування на інцидент.

У РНБО зазначили, що вразливістю Microsoft Exchange найбільше користується китайське кібершпигунське угруповання Hafnium, але вже підтверджена активність й інших хакерських груп. Завдяки вразливості Microsoft

Exchange хакери отримують доступ до серверів, включно з файлами, електронною поштою, обліковими записами, і тому подібне.

«Скомпрометовані сервери також використовуються для розсилок шкідливого програмного забезпечення для подальшого інфікування максимальної кількості організацій. В Україні вже зафіксовано кілька таких інцидентів», – додали у відомстві.

В РНБО зазначили, що вразливими є локальні версії Microsoft Exchange Server 2010, Microsoft Exchange Server 2013, Microsoft Exchange Server 2016, Microsoft Exchange Server 2019. Водночас, інформація щодо вразливостей у хмарних версіях Microsoft 365, Exchange Online, Azure Cloud, відсутня…» ***(Валерій Савицький. В Україні підвищився рівень кіберзагроз через вразливість Microsoft // UA.NEWS (https://ua.news/ua/v-ukrayne-povysylsya-uroven-kyberugroz-yz-za-uyazvymosty-microsoft/). 15.03.2021).***

***

«Україна наклала санкції на чотирьох росіян, які вважаються хакерами Головного розвідувального управління Росії. Відповідний указ сьогодні підписав президент Володимир Зеленський.

Про це йдеться на сайті Офісу президента.

У списку санкцій опинилися Олексій Мінін, Олексій Моренець, Євген Серебряков та Олег Сотніков. Цим громадянам на три роки заборонили в'їзд на територію України та заблокували їх активи.

Федеральне бюро розслідувань США вважає Серебрякова старшим офіцером ГРУ. На думку західних спецслужб, він брав участь в серії хакерських атак та, можливо, керував іншими хакерськими мобільними групами. Зокрема, його підозрюють в причетності до хакерської атаки в Ріо-де-Жанейро під час проведення Олімпійських ігор.

Моренця також називають офіцером ГРУ. ФБР вважає, що він відповідав за перевезення та підготовку обладнання для хакерських атак. Моренця підозрюють в участі в спробах злому Міжнародного олімпійського комітету, WADA та Організації із заборони хімічної зброї.

Сотніков та Мінін, яких також вважають офіцерами ГРУ, допомагали Серебрякову та Моренцю у спробі злому мережі Організації із заборони хімічної зброї в Гаазі. У 2018 році їх затримали та вислали з Нідерландів…». ***(Дмитро Левицький. Зеленський ввів санкції проти російських хакерів з ГРУ // РБК-Україна (https://www.rbc.ua/ukr/news/zelenskiy-vvel-sanktsii-protiv-rossiyskih-1616529749.html). 23.03.2021).***

***

Боротьба з кіберзлочинністю в Україні

«Протиправну діяльність викрили працівники Департаменту кіберполіції спільно із слідчим управлінням столичної поліції та Службою безпеки України.

Фігуранти розсилали на електронні адреси компаній та підприємців листи зі шкідливим програмним забезпеченням. Повідомлення маскували під архіви з документами, в яких були вимоги оплати певних послуг чи надання інформації державним органам.

Вірусні програми надавали віддалений доступ до комп'ютерів бухгалтерів та директорів. Зловмисники створювали платіжні доручення від імені юридичних та фізичних осіб на підконтрольні рахунки. У подальшому гроші обготівковували.

За попередніми підрахунками, потерпілим нанесено понад 5 мільйонів гривень збитків.

Правоохоронці провели вісім обшуків на території Києва та Київської області. Вилучили комп'ютерну техніку, мобільні телефони, банківські картки, флеш-накопичувачі та «чорнові» записи.

Відкрито кримінальне провадження за ч. 3 ст. 185 (Крадіжка), ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) ч. 3 ст. 190 (Шахрайство) Кримінального кодексу України. Зловмисникам може загрожувати до восьми років позбавлення волі. Слідчі дії тривають.

Процесуальне керівництво у кримінальному провадженні здійснює Київська міська прокуратура». ***(Кіберполіція викрила групу зловмисників, які за допомогою «вірусу» викрали понад 5 мільйонів гривень // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-grupu-zlovmysnykiv-yaki-za-dopomogoyu-virusu-vykraly-ponad--miljoniv-gryven-8436/). 15.03.2021).***

***

«Працівники кіберполіції в Одеській області спільно зі слідчими поліції викрили хакера у розповсюдженні шкідливого програмного забезпечення.

Кіберполіція встановила, що 24-річний місцевий мешканець власноруч розробив та розповсюджував шкідливе програмне забезпечення. Програма давала змогу віддаленого зламу адміністративних панелей вебресурсів. В результаті фігурант отримував наявні в таких панелях відомості про користувачів, зокрема їх персональні дані, банківські реквізити, дані для входу до інтернет-банкінгу, акаунтів соцмереж, електронних скриньок тощо.

Хакер зашифровував шкідливе програмне забезпечення у документи в форматі pdf та розсилав на електронні скриньки користувачам поштових сервісів. Для цього він видавав себе за представника служби безпеки сервісів. Свою розробку чоловік також продавав на хакерських форумах та у месенджері.

В оселі правопорушника працівники поліції провели санкціонований обшук. Вилучено мобільні телефони та комп'ютерну техніку. В ході попереднього огляду вилученої техніки, кіберполіцейські виявили зразки вірусного програмного забезпечення, близько 15 мільйонів дискредитованих логінів та паролів до різних систем інтернет-банкінгу, банківські реквізити користувачів та списки авторизаційних даних до вебпанелей.

Фігуранту оголошено про підозру за ч. 1 ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних

засобів, а також їх розповсюдження або збут) Кримінального кодексу України. Підозрюваному може загрожувати до двох років позбавлення волі. Слідство триває.

Процесуальне керівництво здійснює Одеська місцева прокуратура». ***(Кіберполіція викрила одесита у створенні та розповсюдженні шкідливого програмного забезпечення // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-odesyta-u-stvorenni-ta-rozpovsyudzhenni-shkidlyvogo-programnogo-zabezpechennya-1768/). 10.03.2021).***

***

«Правопорушення викрили співробітники Департаменту кіберполіції спільно з Головним слідчим управлінням Нацполіції.

Встановлено, що до таких дій причетні працівники столичного товариства, які надавали комунікаційні послуги під виглядом IP-телефонії. В одному з офісних центрів правопорушники розмістили спеціалізоване телекомунікаційне обладнання, в якому використовувалося до тисячі sim-карток українських операторів мобільного зв'язку.

Обладнання було налаштоване на прийом вхідних викликів з-за кордону з подальшим перенаправленням під виглядом псевдонаціональних в обхід Міжнародного центру комутації. Таким чином міжнародні виклики тарифікувались за цінами національних.

Попередньо встановлено, що стільниковим операторам завдано понад пів мільйона гривень збитків.

Правоохоронці провели обшуки в трьох офісах компанії. За результатами вилучено комп'ютерну техніку, стартові пакети, мобільні телефони, спеціалізоване телекомунікаційне обладнання.

За даним фактом відкрито кримінальне провадження за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України. Санкція статті передбачає до шести років позбавлення волі.

Процесуальне керівництво здійснює Офіс Генерального прокурора України». ***(Кіберполіцейські викрили працівників товариства у несанкціонованому втручанні в роботу операторів стільникового зв'язку // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpoliczejski-vykryly-praczivnykiv-tovarystva-u-nesankczionovanomu-vtruchanni-v-robotu-operatoriv-stilnykovogo-zvyazku-2489/). 01.03.2021).***

***

«У Києві СБУ припинила роботу ботоферми, через яку розповсюджували фейкову інформацію про Україну. Її діяльність фінансували з Росії.

Зловмисники розмістили обладнання у одній із київських квартир. Вони створювали і просували фейкові акаунти у соцмережах, звідки поширювали неправдиву інформацію серед населення.

Спотворена інформація повинна була поширювати негативні настрої у суспільстві та підірвати довіру до української влади всередині країни та за кордоном.

Спецслужба встановила, що загальна кількість фейкових акаунтів становила понад 5 тис. А фігуранти діяли в інтересах тих осіб, які підтримували війну проти України.

Окрім цього, для своєї діяльності вони використовували українські SIM-карти.

Під час обшуків правоохоронці вилучили комп'ютерну техніку зі спеціалізованим програмним забезпеченням, телекомунікаційне обладнання та понад 3 тис. SIM-карток…» ***(Анастасія Рогожінська. Поширювали фейки про Україну: СБУ викрила ботоферму, яку фінансувала РФ // ФАКТИ. ICTV (https://fakty.com.ua/ua/proisshestvija/20210319-poshyryuvaly-fejky-pro-ukrayinu-sbu-vykryla-botofermu-yaku-finansuvala-rf/). 19.03.2021).***

***

«Киберполиция задержала 24-летнего мужчину, который взламывал аккаунты и воровал чужие пароли. Хакер собрал базу из около 15 млн дискредитированных логинов и паролей…

Отмечается, что злоумышленник разработал и распространял вредоносное программное обеспечение, которое позволяло ему удаленно взламывать административные панели веб-ресурсов. В результате хакер получал их персональные данные пользователей, банковские реквизиты, данные для входа в интернет-банкинг, данные аккаунтов соцсетей, электронной почты и т.д.

«Хакер зашифровывал вредоносное программное обеспечение в документе в формате pdf и рассылал на электронные ящики пользователей почтовых сервисов. Для этого он выдавал себя за представителя службы безопасности сервисов. Свою разработку мужчина также продавал на хакерских форумах и в мессенджере», - говорится в сообщении.

Правоохранители провели обыск по месту проживания злоумышленника, в ходе которого изъяли мобильные телефоны и компьютерную технику. Также киберполицейские обнаружили образцы вирусного программного обеспечения, около 15 миллионов дискредитированных логинов и паролей к различным системам интернет-банкинга, банковские реквизиты пользователей и списки авторизационных данных вебпанелей.

Уголовное производство открыто по ч. 1 ст. 361-1 (создание с целью использования, распространения или сбыта вредных программных или технических средств, а также их распространение или сбыт) Уголовного кодекса Украины. Мужчине грозит до двух лет лишения свободы…». ***(Украл пароли у 15 млн человек: в Одесской области задержали хакера // Аргументы и факты (https://aif.ua/society/law/ukral_paroli_u_15_mln_chelovek_v_odesskoy_oblasti_zaderzhali_hakera). 18.03.2021).***

***

«Специалисты по кибербезопасности Службы безопасности Украины заблокировали незаконную схему, которую организовали чиновники госструктур. Они продавали заказчикам информацию силовых ведомств с ограниченным доступом.

Оперативники спецслужбы задокументировали, что участники группы систематически "снимали" информацию из баз данных подразделений Министерства внутренних дел, Государственной миграционной, налоговой и пограничной служб.

Что узнали специалисты СБУ

Похищенную информацию с ограниченным доступом злоумышленники продавали заказчикам.

СБУ задокументировала причастность к этой организации сотрудников правоохранительных органов и структур контроля.

В рабочих кабинетах и домах злоумышленников провели 6 обысков – в Киевской, Херсонской и Кировоградской областях.

Что изъяли в ходе следственных действий

ноутбуки;

банковские карточки;

распечатки незаконных выдержек из баз данных;

и другие носители доказательств противоправной деятельности.

Какие дальнейшие шаги правоохранителей

Продолжается досудебное следствие в рамках уголовного производства. Сейчас устанавливают людей, причастных к организации незаконной схемы». ***(Продавали секретную информацию силовых ведомств: СБУ разоблачила группу чиновников // Телеканал новостей «24» (https://novyny.24tv.ua/ru/prodavali-sekretnuju-informaciju-sbu-razoblachila-novosti-herson_n1572518). 18.03.2021).***

***

«39-річний житель Тернопільщини підозрюється у розробці фішингового пакету і спеціальної адміністративної панелі до нього, які були націлені на вебресурси понад сотні банківських установ та їх клієнтів у країнах Європи та Австралії. Адмінпанель дозволяла контролювати облікові записи користувачів, які зареєструвалися на скомпрометованих ресурсах та вводили свої платіжні дані. Надалі ці дані використовували хакерські угруповання у власних цілях.

За результатами комп'ютерно-технічних експертиз виявлено сотні різноманітних шкідливих програмних продуктів, які демонстрував та продавав фігурант у власному інтернет-магазині у Darknet. Збитки від протиправної діяльності сягають десятків мільйонів доларів.

Фігуранту повідомлено про підозру за ч. 2. ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України. Підозрюваному загрожує до п’яти років позбавлення волі з конфіскацією програмних чи технічних засобів. Досудове розслідування триває.

Процесуальне керівництво здійснює Офіс Генерального прокурора України». ***(Хакеру, який розробив один із найбільших у світі фішингових сервісів для атак на фінустанови, повідомлено про підозру – Нацполіція // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/xakeru-yakyj-rozrobyv-odyn-iz-najbilshyx-u-sviti-fishyngovyx-servisiv-dlya-atak-na-finustanovy-povidomleno-pro-pidozru---naczpolicziya-6626/). 29.03.2021).***

***

Міжнародне співробітництво у галузі кібербезпеки

«Прем'єр-міністр України Денис Шмигаль пропонує Німеччині обмін досвідом у сфері кібербезпеки, оскільки Україна постійно протистоїть кібератакам з боку Російської Федерації.

…про це Шмигаль сказав під час зустрічі з федеральним міністром оборони Німеччини Аннегрет Крамп-Карренбауер.

Зустріч відбулася в рамках робочого візиту української делегації до Федеративної Республіки Німеччина.

Сторони порушили питання безпекової ситуації на сході України та деокупації Криму.

Прем'єр-міністр України наголосив, що Україна зацікавлена в активізації військово-технічного співробітництва з ФРН як з одним із важливих міжнародних партнерів.

Шмигаль запропонував Крамп-Карренбауер обмін досвідом у сфері кібербезпеки, оскільки Україна постійно протистоїть кібератакам з боку Російської Федерації. «Україна, фактично будучи полігоном для застосування кіберінструментів із зловмисною метою, має унікальний практичний досвід з нейтралізації кібератак, який може бути корисним для держав-партнерів», — зауважив очільник уряду.

Прем'єр-міністр підкреслив, що Україна прагне розвивати співробітництво з ФРН у сфері кібербезпеки, і на даному етапі важливим є поглиблення секторальної співпраці. У зв'язку з цим Україна, як відзначив Шмигаль, зацікавлена у проведенні другого раунду двосторонніх кіберконсультацій з Німеччиною.

Прем'єр-міністр України запевнив міністра оборони Німеччини, що євроатлантична інтеграція є пріоритетом зовнішньої політики та політики безпеки України. Він також подякував Німеччині за підтримку в питанні надання Україні статусу партнера НАТО з розширеними можливостями.

«Україна використовуватиме цей статус для подальшого зміцнення відносин з Альянсом. Зокрема ми прагнемо досягти цього через збільшення участі в операціях, тренуваннях та навчаннях НАТО, через посилення обміну інформацією між Україною та Альянсом, обміну досвідом та знаннями щодо протидії гібридній війні та через збільшення присутності українських спеціалістів на посадах в структурах НАТО», — відзначив Прем'єр-міністр…». ***(Шмигаль пропонує Німеччині обмін досвідом у сфері кібербезпеки // Укрінформ***

(https://www.ukrinform.ua/rubric-polytics/3211319-smigal-proponue-nimeccini-obmin-dosvidom-u-sferi-kiberbezpeki.html). 19.03.2021).

***

«Завершився робочий візит Прем'єр-міністра України Дениса Шмигаля до Німеччини, під час якого він відвідав не лише Берлін, а й столицю землі Північний Рейн-Вестфалія Дюссельдорф.

Власне, там відбулася ключова зустріч з наступником нинішньої канц-лерки Ангели Меркель, головою Християнсько-демократичного союзу і прем'єр-міністром Північного Рейну-Вестфалії Арміном Лашетом. Як повідомляє «Урядовий портал», під час переговорів йшлося про міжрегіональне співробітництво, зокрема про саміт «Кримської платформи». Також у Дюссельдорфі український прем'єр зустрівся з представниками місцевого уряду, за його присутності було підписано Меморандум про взаєморозуміння стосовно налагодження українсько-німецького партнерства у сфері діджиталізації. Серед важливих зустрічей у Берліні варто відзначити перемовини з федеральним міністром оборони Німеччини Аннегрет Крамп-Карренбауер, під час яких ішлося про поглиблення військово-технічного співробітництва з ФРН. Особливий акцент було зроблено на необхідності обміну досвідом у сфері кібербезпеки». ***(Денис Шмигаль провів зустріч з наступником Меркель // Голос України (http://www.golos.com.ua/article/343522). 20.03.2021).***

***

«Безпека буває різною, не тільки пов'язаної зі зброєю. Коли йдеться про розширення складової безпеки в рамках Східного партнерства, представник України при ЄС Микола Точицький хотів би згадати про те, що в травні 2020 року Єврокомісія включила в перелік співпраці також протидія тероризму і готовність протистояти гібридним загрозам.

"Вважаю, що відкриття нових можливостей для освіти у сфері безпеки — це теж практичний елемент, який зміцнить безпекову інфраструктуру", - пише дипломат у статті.

Він підкреслив, що поступове залучення до інформаційної та кібербезпекової політики ЄС дасть країнам Східного партнерства можливість отримати досвід у сфері аналітики чи практик протидії та ефективніше реагувати на наднаціональні загрози як для країн Тріо Східного партнерства – України, Грузії, Молдови, – так і для Євросоюзу…». ***(Україна може допомагати ЄС в сфері безпеки – Точицький // Дзеркало тижня. Україна (https://zn.ua/ukr/POLITICS/ukrajina-mozhe-dopomahati-jes-v-sferi-bezpeki-tochitskij.html). 23.03.2021).***

***

«США будут способствовать всестороннему прогрессу в укреплении кибербезопасности Украины, заявляет представитель Посольства США в Украине Адам Марлоу.

…об этом он сказал во время второго заседания Национального кластера по кибербезопасности.

Заседание в рамках продолжения сотрудничества между Национальным координационным центром кибербезопасности (НКЦК) при Совете национальной безопасности и обороны Украины и Фондом гражданских исследований и развития Соединенных Штатов Америки (CRDF Global) (при поддержке Государственного департамента США) состоялось в формате Zoom-конференции и было посвящено обсуждению проекта новой Стратегии кибербезопасности Украины на 2021-2025 годы.

Руководитель службы по вопросам информационной безопасности и кибербезопасности Аппарата СНБО Украины Наталья Ткачук поблагодарила всех стейкхолдеров, привлеченных к разработке Стратегии, и сообщила, что проект Стратегии был вынесен для общественного обсуждения, которое вскоре завершится.

По ее словам, проект получил положительную оценку со стороны представителей общественности Украины, а также партнеров из стран-членов Евросоюза, Великобритании, США. По результатам обработки этих предложений в конце марта проект Стратегии будет финализирован.

Ткачук отметила, что одной из важных задач является подготовка пятилетней дорожной карты, которая будет детализирована Кабинетом Министров Украины путем утверждения ежегодных планов по реализации Стратегии.

Руководитель управления обеспечения деятельности НКЦК Аппарата СНБО Украины Сергей Прокопенко напомнил, что основой для работы стало утверждение Президентом в сентябре 2020 г. Стратегии национальной безопасности Украины. 12 октября прошлого года Глава государства поручил НКЦК разработать проект Стратегии кибербезопасности Украины и подать его в шестимесячный срок на рассмотрение СНБО Украины.

Заместитель председателя Комитета Верховной Рады Украины по вопросам цифровой трансформации Александр Федиенко сообщил, что в парламенте зарегистрированы два законопроекта по защите критической инфраструктуры Украины (правительственный и авторства народных депутатов).

По его словам, в последние годы в Украине сделаны шаги к улучшению нормативно-правовой базы в сфере кибербезопасности, однако необходимо прилагать усилия к ее дальнейшему совершенствованию.

Представитель Посольства США в Украине Адам Марлоу поблагодарил ключевые заинтересованные стороны за сотрудничество и отметил, что США «непреклонны в поддержке Украины в сфере кибербезопасности и ожидают, что благодаря Национальному кластеру реформирование этой сферы будет продолжено». США, в свою очередь, будут способствовать всестороннему прогрессу в укреплении кибербезопасности Украины, отметил он.

Заместитель руководителя Программы кибербезопасности CRDF Global в Украине Михаил Верич представил основную цель, цели и приоритеты Национального кластера кибербезопасности. По его словам, это «инициатива коалиции, сотрудничества и координационная площадка для субъектов национальной системы кибербезопасности, министерств и других государственных органов и неправительственных институтов, представителей посольств, донорских организаций, частного сектора, международных партнеров ради эффективной

совместной работы в реализации ряда программ и проектов по кибербезопасности в Украине».

Следующее заседание планируется провести 29 апреля…». ***(США будут способствовать укреплению кибербезопасности Украины – посольство // Укринформ (https://www.ukrinform.ru/rubric-polytics/3216127-ssa-budut-sposobstvovat-ukrepleniu-kiberbezopasnosti-ukrainy-posolstvo.html). 26.03.2021).***

***

«Новоназначенный чрезвычайный и полномочный посол Украины в США Оксана Маркарова считает, что США могут набраться у Украины эффективного опыта противодействия киберугрозам…

"Мы точно могли бы быть не просто площадкой для изучения, но и стать активным участником, лидером определенного международного или совместного украинского-американского центра", - рассказала об амбициозных планах посол.

По ее словам, Украина может стать экспертом в этой отрасли по нескольким причинам. Все дело в том, что, начиная с 2015 года Украина несколько раз подвергалась критическому влиянию из вне, причем по большей части, на объекты критической инфраструктуры.

"Состоялись кибернападения на наш финансовый сектор, когда под угрозой оказалась инфраструктура всех государственных банков", - уточнила Маркарова.

После этого, как уточнила представитель Украины в США, государству пришлось научиться ставить предохранители.

"Мне кажется, о кибербезопасности Украина может многое поведать миру. Мы здесь не будем просить о помощи, а сами готовы предоставлять ее другим", - уверена она.

Также Маркарова подчеркнула, что Зеленский уже публично объявил о создании выше указанного центра по итогам недавнего заседания Совета национальной безопасности и обороны (СНБО)…». ***(Наталия Гурковская. Новая посол нашла, чему Украина может научить США // Телеграф (https://telegraf.com.ua/ukraina/politika/5619466-novaya-posol-nashla-chemu-ukraina-mozhet-nauchit-ssha.html). 15.03.2021).***

***

«Европа и Соединенные Штаты воспользуются потеплением в отношениях, чтобы заключить пакт, который позволит обмениваться частными данными через Атлантику, заменив предыдущие соглашения, отмененные судом ЕС.

Facebook, Google, Microsoft и тысячи других компаний хотят заключить такую сделку, чтобы интернет-трафик не прерывался, не подвергаясь серьезной юридической опасности из-за европейских законов о конфиденциальности.

В прошлом году Европейский суд «поднял важные вопросы о том, как обеспечить защиту конфиденциальности, когда данные пересекают Атлантику», - сказал комиссар юстиции ЕС Дидье Рейндерс в своем выступлении в Американской торговой палате перед ЕС.

«Поиск этого решения является приоритетом для Брюсселя и Вашингтона», - добавил он через день после активизации переговоров с министром торговли США Джиной Раймондо.

Как «партнеры-единомышленники», обе стороны «должны быть в состоянии найти подходящие решения по принципам, которые ценятся по обе стороны Атлантики», - сказал он.

Третья попытка нового порядка данных увенчалась успехом в сделках, которые были признаны недействительными после успешных судебных процессов, в которых утверждалось, что законы о безопасности США нарушают основные права граждан ЕС.

Правовое наступление возглавил Макс Шремс, австрийский активист и юрист, который начал свою кампанию после того, как Эдвард Сноуден разоблачил массовый цифровой шпионаж со стороны агентств США.

С тех пор компании прибегают к юридически неопределенным обходным путям, чтобы поддерживать поток данных, в надежде, что обе стороны смогут придумать что-то более сильное в долгосрочной перспективе.

Рейндерс сказал, что сделка потребует решения «сложных и деликатных» вопросов, «относящихся к хрупкому балансу между национальной безопасностью и конфиденциальностью».

Сделка должна будет охватывать важные вопросы, включая гарантии доступа к судам и четко обеспеченные права личности.

«Единственный способ добиться этого - разработать новую договоренность, которая полностью соответствует решению (суда ЕС) Schrems II. Это в наших общих интересах», - добавил Рейндерс.

ЕС заключил аналогичные соглашения с 12 организациями и странами, включая Японию, Швейцарию, Канаду, Израиль, и находится в процессе завершения переговоров с Южной Кореей…». ***(EU, US Make New Attempt for Data Privacy Deal // Wired Business Media (https://www.securityweek.com/eu-us-make-new-attempt-data-privacy-deal). 26.03.2021).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Спустя год после того, как COVID-19 был официально признан пандемией, методы и тактика, используемые киберпреступниками, резко изменились.

Фишинговые электронные письма, связанные с COVID-19, атаки методом грубой силы на удаленных сотрудников и ориентация на использование или злоупотребление платформами для совместной работы являются отличительными чертами киберпреступного предприятия, поскольку коронавирус отмечает свою первую годовщину выхода на мировой уровень.

Спустя год после того, как кризис COVID-19 был официально признан пандемией, образ жизни и работы людей радикально изменился, а также «методы и

тактики, используемые преступниками в Интернете, стремящимися использовать массовый рост онлайн-трафика.

Фишинговые мошенничества используют темы COVID-19

По словам «Лаборатории Касперского», мошенничество с электронной почтой (и, в частности, фишинг) по-прежнему остается одним из самых эффективных видов атак в эпоху коронавируса, поскольку страх и тревога - две из наиболее часто используемых эмоций для такого рода атак социальной инженерии.

Кампании, подобные тем, что предлагали маски N95 или дезинфицирующее средство для рук (которые побуждали людей указывать платежные реквизиты), стали в течение года повсеместными. Выдача себя за власти COVID-19 также была уловкой, когда киберпреступники предлагали «важные» обновления. На самом деле все, что они предлагали, было вредоносным.

Киберпреступники также использовали приманки, связанные с задержкой доставки, пользуясь тем фактом, что количество заказов по почте резко возросло во время блокировки. По данным Kaspersky, в 2020 году службы доставки вошли в десятку организаций, наиболее часто подвергающихся фальсификации для подобных атак.

Атаки грубой силы на удаленных сотрудников

Поскольку в 2020 году миллионы сотрудников были отправлены домой для удаленной работы, для многих организаций меры кибербезопасности стали второстепенными. Согласно анализу, киберпреступники, подозревая это, атаковали сотрудников, которые входили в корпоративные ресурсы с личных устройств и из незащищенных домашних сетей.

В частности, атаки методом перебора (когда злоумышленники пробуют случайные имена пользователей и пароли для учетных записей) на соединениях по протоколу удаленного рабочего стола (RDP) увеличились во всем мире, увеличившись на 197 процентов с 93,1 миллиона во всем мире в феврале до 277,4 миллиона в марте. RDP - это проприетарный протокол Microsoft, который позволяет пользователям получать доступ к рабочим станциям или серверам Windows.

«RDP - один из самых популярных протоколов удаленного доступа, используемых компаниями, что делает его излюбленной целью для злоумышленников», - говорится в отчете. «Весной 2020 года количество атак методом перебора по протоколу RDP резко возросло почти по всей планете».

Спустя год количество атак не вернулось к допандемическому уровню, отмечает Касперский: в феврале было 377,5 миллиона атак методом перебора.

Кибератаки на платформы для совместной работы усиливаются

Кибератаки также преследовали пользователей различных облачных сервисов, особенно сервисов для совместной работы, таких как Flock, GotoMeeting, HighFive, Join.me, Lifesize, MS Teams, Slack, Webex и Zoom. Kaspersky обнаружил, что к маю прошлого года среднесуточное количество атак на эти сервисы, обнаруженное в его телеметрии, подскочило на 25 процентов только с февраля 2020 года.

Они тоже не утихли

По словам Касперского, количество веб-атак после снижения летом 2020 года достигло нового пика в декабре, поскольку большая часть мира столкнулась со второй волной пандемии. «Большая часть времени пользователей, проводимых в сети, была посвящена виртуальным встречам и совместной работе. Вот почему приложения для встреч и обмена сообщениями, такие как Zoom и Teams, стали популярной приманкой для распространения киберугроз».

В большинстве этих атак вредоносные файлы распространяются под видом названий этих приложений. «Лаборатория Касперского» обнаружила, что в январе было обнаружено 1,15 миллиона таких файлов - максимальное количество с момента начала блокировки.

«Эти файлы часто входят в состав, казалось бы, законных установщиков приложений, с которыми можно столкнуться несколькими способами: через фишинговые электронные письма, утверждающие, что они получают уведомления или специальные предложения от их платформ, или через фишинговые веб-страницы», - говорится в отчете.

Что дальше?

Касперский предупредил, что с переходом пандемии в новую фазу, связанную с вакцинацией, фишеры и мошенники могут использовать новые темы, такие как паспорта здоровья для путешествий или распространение вакцины.

«Важно, чтобы пользователи скептически относились к любому электронному письму или веб-сайту, где упоминается пандемия. Более того, недавние события показали, насколько преступники готовы воспользоваться кризисом, и, хотя эта пандемия утихнет, это определенно не будет последним кризисом».

В отчете также отмечается, что удаленная работа, вероятно, сохранится даже после пандемии.

«RDP никуда не денется, как и атаки на протокол», - говорится в отчете. «Это означает, что компаниям необходимо пересмотреть свое использование RDP и узнать, как защитить удаленный доступ. Если у компаний когда-либо было время переоценить и укрепить свою стратегию безопасности, то это время пришло».

(Tara Seals. Cyberattacks See Fundamental Changes, A Year into COVID-19 // Threatpost (https://threatpost.com/cyberattacks-fundamental-changes-covid-19/164775/). 15.03.2021).

***

«Команда специалистов из Университета Квинсленда, Университета Мельбурна и Массачусетского технологического института в США совместно разработала виртуальный «вирус», который потенциально может быть использован для более точной оценки распространения коронавирусной инфекции (COVID-19) и быстрой постановки диагноза.

Решение, получившее название Safe Blues, использует технологию Bluetooth для передачи виртуальных «вирусоподобных» цепочек между мобильными устройствами, имитируя распространение инфекции COVID-19 в сообществе в режиме реального времени. Затем с помощью искусственного интеллекта

виртуальные заражения Safe Blues сравнивают с последними реальными данными о COVID-19.

«Safe Blues распространяет безопасные виртуальные «вирусоподобные» токены, которые реагируют на директивы о социальном дистанцировании так же, как и сам вирус. Токены распространяются через Bluetooth и измеряются в online-режиме», — пояснили эксперты.

По словам исследователей, взаимосвязь между количеством цепочек заражений токенами и развитием реальной эпидемии может быть определена с помощью методов машинного обучения, применяемых для отсроченного измерения фактической эпидемии. Это затем позволяет использовать данные о токенах Safe Blues в режиме реального времени для оценки текущей эпидемии.

Исследователи отметили, что хоть Safe Blues и похоже на приложения для отслеживания контактов с больными COVID-19, его цель «совершенно иная», поскольку решение «не записывает и не хранит информацию о людях и их взаимодействиях с целью отображения конкретных контактов». ***(Передающийся по Bluetooth вирус поможет в оценке распространения COVID-19 // SecurityLab.ru (https://www.securitylab.ru/news/517476.php). 16.03.2021).***

***

«По данным Palo Alto Networks, киберпреступники безжалостно использовали пандемию коронавируса для создания фишинговых веб-сайтов, которые выдавались за Pfizer, BioNTech и других известных поставщиков вакцин и СИЗ.

В опубликованном сегодня сообщении подразделение по разведке угроз Unit 42 Пало-Альто сообщило, что URL-адреса фишинговых приманок на тему COVID «в основном сосредоточены на средствах индивидуальной защиты (СИЗ) и наборах для тестирования в марте 2020 года, правительственных программах стимулирования с апреля по лето 2020 года (включая поддельные Веб-сайт торговой комиссии США, который выдавал себя за Федеральную торговую комиссию США с целью кражи учетных данных пользователей) и вакцины с конца осени 2020 года".

Он добавил, что в период с января 2020 года по январь 2021 года он видел 69 950 фишинговых URL-адресов, которые были посвящены «темам, связанным с COVID». Схемы государственной поддержки были большой темой в первом квартале 2020 года, достигнув пика в мае и заканчивавшись, когда популярность наживки на тему больниц стала расти.

Исследователи Unit 42 обнаружили, что последний включал в себя «поддельный веб-сайт Pfizer и BioNTech, также ворующий учетные данные пользователей». Эти данные в целом совпадают с выводами, сделанными год назад Национальным бюро по расследованию мошенничества британской полиции.

В подразделении 42 подсчитали, что Microsoft была наиболее выдаваемым брендом, на который нацелены фишинговые преступники: страницы на тему Редмонда были созданы для кражи учетных данных сотрудников американской продуктовой фирмы Walgreens, канадского производителя лекарств Pharmascience,

индийской Glenmark Pharmaceuticals и многих других, включая китайскую фармацевтическую фирму.

Microsoft этого не сделала; в июле компания подала иск в США, чтобы получить контроль над фишинговыми доменами.

По словам компании, большинство этих приманок пытались украсть «бизнес-учетные данные» пользователей, заявив: «Эти попытки фишинга, связанные с бизнесом, становятся все более важным вектором атак для киберпреступников».

Фишинговый сайт, созданный позже в 2020 году, представлял собой корпоративное присутствие для производителей вакцин BioNTech и Pfizer, предлагая пользователям войти в систему с учетными данными Office 365, чтобы зарегистрироваться для вакцинации.

«Мы прогнозируем, что по мере продолжения развертывания вакцины фишинговые атаки, связанные с распространением вакцины, в том числе атаки, нацеленные на отрасли здравоохранения и биологии, будут продолжать расти во всем мире», - говорится в сообщении блога Unit 42.

Компания также сообщила, что количество кибератак на аптеки и больницы увеличилось на 189%, многие из которых являются частью более крупных фишинговых кампаний. По словам Unit 42, это были бессистемные попытки получить кредиты для входа в систему, утверждая, что в основном они делались «в надежде, что хотя бы один из сотрудников по ошибке введет свои учетные данные на поддельную страницу входа».

В прошлом году компания Mimecast, занимающаяся безопасностью электронной почты, предупредила о мошенничестве с возмещением стоимости авиабилетов на тему COVID, а GitLab решила проблему, протестировав уязвимость своих сотрудников к фишингу. Последний был обеспокоен; на это попалась примерно пятая часть сотрудников технической фирмы». ***(Gareth Corfield. Scammers tried slurping folks' login details through 70,000 coronavirus-themed phishing URLs during 2020 // The Register (https://www.theregister.com/2021/03/24/covid_phishing_2020_palo_alto_networks_research/). 24.03.2021).***

***

Світові тенденції в галузі кібербезпеки

«Киберустойчивость может рассматриваться как превентивная мера по противодействию человеческой ошибке, злонамеренным действиям, испорченному и небезопасному программному обеспечению.

Когда дело доходит до кибербезопасности, утечки данных, такие как атака цепочки поставок SolarWinds, ясно дали понять одно: сегодняшние атаки больше не ограничиваются простым распространением вируса или атакой типа «отказ в обслуживании» (DoS). Вместо этого киберпреступники применяют сложные постоянные угрозы (APT), угрожая направить их на даже хорошо защищённые и контролируемые инфраструктуры. Быстрый переход к распределенной рабочей силе в ответ на пандемию COVID-19 обострил и без того сложную ситуацию,

расширив ранее существовавшие пробелы в видимости, подотчетности и устойчивости мер безопасности в ИТ-отделах. Неудивительно, что всё больше и больше руководителей по информационной безопасности говорят о киберустойчивости как о новой мере для обеспечения непрерывного выполнения бизнес-операций. Но что такое киберустойчивость и как она соотносится с традиционными методами кибербезопасности?

Определение киберустойчивости

По мнению MITER, киберустойчивость «это способность предвидеть, противостоять, восстанавливаться и адаптироваться к неблагоприятным условиям, стрессам, атакам или компрометациям киберресурсов». Потребность в киберустойчивости возникает из-за растущего осознания того, что традиционных мер безопасности уже недостаточно для страхования достаточной информации, данных и сетевой безопасности. Киберустойчивость признает, что современные корпоративные инфраструктуры состоят из крупных и сложных объектов, поэтому всегда будут иметь недостатки и слабости, которые злоумышленники смогут использовать. В этом контексте цель киберустойчивости состоит в том, чтобы гарантировать, что неблагоприятное кибер-событие (преднамеренное или непреднамеренное, т. е. из-за неудачных обновлений программного обеспечения) не повлияет отрицательно на конфиденциальность, целостность и доступность бизнес-операций организации.

Кибербезопасность применяет технологии, процессы и меры, предназначенные для защиты систем (например, серверов, конечных точек), сетей и данных от кибератак. Киберустойчивость же фокусируется на детективном и реактивном контроле в ИТ-среде организации для оценки пробелов и стимулирования улучшения общего состояния безопасности. Большинство мер киберустойчивости используют или усиливают различные меры кибербезопасности. Меры кибербезопасности и киберустойчивости наиболее эффективны при совместном применении.

Всё больше и больше структур управления киберрисками и безопасностью принимают концепцию киберустойчивости. Например, Обзор киберустойчивости (CRR) Министерства внутренней безопасности предлагает руководство по оценке операционной устойчивости и методов кибербезопасности организации. Другой пример - специальная публикация 800-160 Тома 2 Национального института стандартов и технологий (NIST), которая предлагает основу для разработки безопасных и надежных систем, рассматривая неблагоприятные кибер-события как проблемы устойчивости и безопасности.

Различные варианты киберустойчивости

Как и Zero Trust, киберустойчивость применяется к постоянно растущему диапазону атак и, следовательно, включает такие киберресурсы, как:

- Сети;
- Данные;
- Рабочие нагрузки;
- Устройства;
- Люди (также известные как личности).

Киберресурсы и диапазон неблагоприятных факторов, которым они подвержены, варьируются в зависимости от контекста, в котором требуется киберустойчивость. В любой ситуации приоритет, который организация назначает установлению мер киберустойчивости для различных киберресурсов, должен определяться оценкой тактики, методов и процедур (так называемых ТТП), которые хакеры обычно применяют во время эксплуатации своих жертв.

Например, конечные точки часто используются хакерами и киберпреступниками в качестве точки доступа для запуска атак, которые могут заразить всю сеть организации, или выступать в качестве плацдарма для бокового перемещения внутри сети. Недавний опрос Ponemon Institute показал, что 68% организаций подверглись успешной атаке на конечные точки за последние 12 месяцев. Несмотря на широко распространенные попытки защитить конечные точки, это число свидетельствует о том, что безопасность быстро ухудшается и, следовательно, требует устойчивости конечных точек, что является лишь одним из «вариантов», которые может принимать киберустойчивость. Устойчивость конечных точек позволяет организациям всегда знать их месторасположение, осуществлять глубокий контроль и действия по обеспечению безопасности на этих устройствах, а также помогать своим средствам управления безопасностью восстанавливать себя, когда они отключены, изменены или иным образом скомпрометированы.

Преимущества киберустойчивости

Стратегии киберустойчивости, такие как Endpoint Resilience, предоставляют ряд преимуществ до, во время и после кибератаки. Вот некоторые из основных преимуществ:

• Повышенная безопасность: киберустойчивость не только помогает реагировать на атаки и выжить, а также может помочь организации разработать стратегии для улучшения управления ИТ, повышения безопасности критически важных активов, расширения усилий по защите данных и минимизации ошибок, связанных с человеческим фактором.

• Улучшенное положение соответствия: многие отраслевые стандарты, правительственные постановления и законы о конфиденциальности данных в настоящее время способствуют киберустойчивости.

• Повышение производительности ИТ. Одним из недооцененных преимуществ киберустойчивости является то, что она улучшает повседневные операции ИТ-команды организации, улучшает способность реагировать на угрозы и помогает обеспечить бесперебойную повседневную работу.

Меры киберустойчивости (т. е. архитектурный дизайн, технологии, методы работы) предполагают, что сегодняшние субъекты угроз могут закрепиться в инфраструктуре организации, а действиям после взлома следует препятствовать. При правильном внедрении киберустойчивость может рассматриваться как превентивная мера по противодействию человеческой ошибке, злонамеренным действиям, испорченному и небезопасному программному обеспечению. В конечном итоге цель киберустойчивости - агрессивная защита всего предприятия, охватывающая все вышеупомянутые доступные киберресурсы. Таким образом, предприятиям необходимо создать различные варианты киберустойчивости в своей

инфраструктуре». ***(Torsten George. The Different Flavors of Cyber Resilience // Wired Business Media (https://www.securityweek.com/different-flavors-cyber-resilience). 03.03.2021).***

***

«Vectra AI, поставщик средств обнаружения и реагирования на сети (NDR), опубликовал глобальный опрос 1112 специалистов по безопасности, работающих в средних и крупных организациях, использующих Microsoft Office 365. Результаты подтверждают, что пандемия COVID-19 ускорила миграцию в облако и цифровую трансформацию среди 88% компаний и 71% развертываний Microsoft Office 365 подвергались перехвату учетной записи законного пользователя не один, а в среднем семь раз за последний год.

Тот факт, что 3 из 4 компаний подверглись атакам со злонамеренным захватом учетных записей, подчеркивает необходимость отслеживания и защиты учетных записей при их перемещении из локальной среды в облако. Лишь каждый третий специалист по безопасности считает, что может немедленно выявить и остановить атаку с захватом учетной записи, и большинство ожидает, что на перехват такого взлома уйдут дни или даже недели.

Проблемы, с которыми сталкиваются защитники, отражают результаты последнего отчета Spotlight, в котором отслеживалось поведение четырех миллионов клиентов Microsoft Office 365 в течение 90 дней и было обнаружено, что 96% сетей демонстрируют подозрительное поведение в боковом направлении и что захват учетных записей находится в верхней части списка методов, используемых злоумышленниками для горизонтального перемещения между облаком и сетью.

Тим Уэйд, технический директор группы технического директора Vectra, комментирует: «Мы регулярно видим, как атаки на основе идентификации используются для обхода традиционных средств защиты периметра, таких как многофакторная аутентификация (MFA). Захват аккаунтов заменяет фишинг как наиболее распространенный вектор атаки, а защита от MFA - это лежачие полицейские, а не силовые поля. Организации должны отнестись к этому серьезно и спланировать обнаружение и сдерживание компрометации учетных записей до того, как произойдет существенное нарушение их деятельности - злонамеренный доступ даже на короткий период времени может нанести огромный ущерб».

Однако опрос также показывает высокий уровень уверенности групп безопасности в эффективности мер безопасности их собственной компании: почти 4 из 5 утверждают, что имеют хорошую или очень хорошую видимость атак, которые обходят средства защиты периметра, такие как брандмауэры. Тем не менее, существует интересный контраст во мнениях между респондентами на уровне управления и практиками, такими как аналитики Центра управления безопасностью (SOC), при этом менеджеры демонстрируют гораздо большую уверенность в своих защитных способностях. В целом, основными проблемами безопасности, которые отмечают клиенты Microsoft Office365, являются риск компрометации данных, хранящихся в облаке, риск перехвата учетной записи и способность хакеров использовать наземные атаки, чтобы скрыть свои следы.

Тим Уэйд, технический директор группы технического директора Vectra, комментирует: «Тенденция менеджеров быть значительно более уверенными по сравнению с теми, кто работает на угольном забое, говорит о том, что здесь имеет место уровень самообмана. Возможно, это связано с тем, что метрики, которые передаются высшему руководству, часто больше ориентированы на объем остановленных атак, а не на серьезность атаки или количество расследований. Какой бы ни была причина, важно не останавливаться на достигнутом и постоянно следить за новыми типами атак».

Результаты также показывают, что большинство (58%) специалистов по безопасности говорят, что разрыв между злоумышленниками и защитниками увеличивается. Переход к облаку и внедрение удаленной работы повысили угрозу кибератак: четверо из пяти специалистов по безопасности заявили, что риски кибербезопасности увеличились за последние двенадцать месяцев.

Среди других ключевых выводов отчета:

- Интернет вещей / подключенные устройства и атаки на основе идентификационных данных - две главные проблемы безопасности на 2021 год;
- 58% предприятий планируют инвестировать больше денег в людей и технологии, а 52% будут инвестировать в ИИ и автоматизацию в 2021 году;
- Самое большое разочарование существующими решениями безопасности - это время, необходимое для управления ими…». ***(75% of cloud users suffered up to seven malicious account takeovers in last year // BNP Media (https://www.securitymagazine.com/articles/94837-of-cloud-users-suffered-up-to-seven-malicious-account-takeovers-in-last-year). 17.03.2021).***

***

«Опрос Intel показывает, что большинство организаций предпочитают, чтобы поставщики услуг имели проактивную безопасность, но лишь немногие из них отвечают ожиданиям безопасности.

Почти три четверти опрошенных профессионалов в области ИТ-безопасности (73 процента) заявили, что они предпочитают покупать технологии и услуги у поставщиков, которые проявляют инициативу в отношении безопасности, включая использование этического взлома и прозрачную коммуникацию об уязвимостях. Но поставляют менее половины поставщиков.

Опрос, проведенный Poneman Institute по заказу Intel, был призван помочь лучше понять, что влияет на принятие решений об инвестициях в безопасность. Ponemon Institute опросил 1875 человек в Африке, Европе, на Ближнем Востоке, в Великобритании и США, которые участвуют в ИТ-инфраструктуре своих организаций, а также знакомы с процессами закупок технологий и услуг.

Исследование показывает большой разрыв между ожиданиями лиц, принимающих решения в организации, с точки зрения безопасности, и способностью их поставщиков оправдать эти ожидания. Например, 66% опрошенных заявили, что предпочитают, чтобы бэкдоры имели «возможность выявлять уязвимости в своих собственных продуктах и устранять их». Тем не менее, только 46% тех же респондентов заявили, что их поставщики технологий обладают такой способностью.

30% опрошенных заявили, что они могут исправить уязвимость за неделю или меньше, но в среднем требуется около шести недель, чтобы исправить ошибку с момента ее первого обнаружения, а 63% заявили, что задержки вызваны «человеческой ошибкой».

Но рост числа недостатков нулевого дня, таких как те, которые недавно были обнаружены в программном обеспечении, таком как Google Chrome или Microsoft Exchange, означает, что эти организации могут оставаться уязвимыми для атак на несколько недель, прежде чем будет установлено исправление, в зависимости от поставщика.

«Безопасность не возникает просто так», - сказала Сюзи Гринберг, вице-президент Intel Product Assurance and Security. «Если вы не находите уязвимых мест, значит, вы недостаточно внимательно».

Прозрачность безопасности

Прозрачность в отношении обновлений безопасности и уязвимостей также имела большое значение для предприятий: 64% респондентов отметили, что «возможность прозрачности в отношении доступных обновлений безопасности и средств защиты» является «очень важной». Несмотря на необходимость, только 48% респондентов говорят, что получают такой вид общения.

Подавляющее большинство респондентов - 74% - согласились с тем, что этичный взлом / поиск ошибок для поиска уязвимостей в продуктах «очень важен».

Другие результаты опроса показывают, что организации изо всех сил стараются не отставать от кибербезопасности и обращаются за помощью к поставщикам. В то же время бюджеты ужесточаются: 45% опрошенных заявили, что их бюджеты «менее чем адекватны».

Эти результаты представляют собой моментальный снимок внутри развивающихся ИТ-операций, где до сих пор не ясно, кто несет ответственность за риск для безопасности организации. 21% считают, что это должен быть директор по информационной безопасности, 19% полагают, что ИТ-директор или технический директор по техническим вопросам должны возглавить усилия по обеспечению безопасности, а 17% считают, что ответственность должны нести руководители бизнес-подразделений…

Это неопределенно может предоставить возможность поставщикам, которые готовы помочь ИТ-отделам, испытывающим трудности, взять на себя бремя кибербезопасности.

«Ключевым моментом здесь является прозрачность», - сказал Гринберг. «У организаций есть аппетит к гарантиям безопасности и свидетельствам того, что компоненты работают в известном и надежном состоянии. Как отрасль, мы должны не только оценивать риски, но и следить за тем, чтобы клиенты знали, когда будут доступны обновления безопасности, чтобы укрепить доверие. Наша конечная цель - использовать прозрачный подход к безопасности для защиты рабочих нагрузок клиентов и повышения устойчивости программного обеспечения, и мы призываем наших отраслевых партнеров и конкурентов последовать их примеру». ***(Becky Bracken. Cybersecurity Bug-Hunting Sparks Enterprise Confidence // Threatpost (https://threatpost.com/cybersecurity-bug-hunting-enterprise-confidence/164782/). 15.03.2021).***

***

«Insider Risk Management строит структуру вокруг новой парадигмы «терпимости к риску», стремясь дать командам безопасности видимость и контекст вокруг активности данных для их защиты, не налагая жестких ограничений на пользователей.

Пандемия ускорила цифровую трансформацию предприятия. Это не просто резкая смена удаленной работы - это глубокий сдвиг в сторону приоритета скорости и гибкости как движущих сил конкурентного преимущества компании. Но поскольку более быстрые и гибкие способы работы резко увеличивают риски безопасности данных, исходящие от наших сотрудников, это заставляет задуматься: как вы управляете этими растущими рисками, не снижая скорости и гибкости вашего бизнеса?

Ответ - новая категория технологий защиты данных: управление внутренними рисками (IRM). IRM строит основу вокруг новой парадигмы «терпимости к риску», стремясь предоставить группам безопасности видимость и контекст вокруг активности данных для защиты этих данных, не налагая жестких ограничений на пользователей. Внимание к инсайдерскому риску растет. По данным Gartner, «руководители служб безопасности и управления рисками наблюдают возрастание спроса на оценку и управление внутренними рисками, включая наблюдение за работниками с высоким уровнем риска и мониторинг аномалий критических приложений и данных».

Инсайдерский риск против инсайдерской угрозы

Традиционное представление об инсайдерской угрозе вызывает в воображении мысли о сотрудниках-злоумышленниках, намеренно крадущих ценные данные, или о преднамеренно небрежных сотрудниках, раскрывающих конфиденциальные данные. Проблема в том, что большинство действий сотрудников, которые сегодня ставят под угрозу данные, не попадают ни в одну из этих категорий. Скорее, они являются результатом того, что люди просто выполняют свою повседневную работу и непреднамеренно подвергают данные риску.

Вот где есть различие между внутренней угрозой и внутренним риском: традиционные представления о внутренней угрозе предполагают, что угрозы являются окончательными и должны быть остановлены или заблокированы. Но изобретательность и новаторское решение проблем - это не то поведение, которому следует препятствовать… Итак, новая парадигма управления внутренними рисками основана на понимании нюансов риска, а не на его предотвращении.

Это не блокирует

Важным элементом смены парадигмы в мире безопасности данных является то, что IRM не верит в «блокировку». Традиционные подходы к предотвращению внутренних угроз обычно основываются на инструментах блокировки на основе политик, чтобы остановить определенный набор угроз. Но из-за отсутствия простого и четкого разграничения между тем, что действительно угрожает, и тем, что просто повседневная работа, ясно, что командам безопасности нужен новый подход для снижения рисков безопасности данных. Вместо блокировки Gartner

определяет трехэтапный подход: «в первую очередь удерживать людей от желания делать это; Обнаружить активность; увеличить усилия». Организации должны:

Определять - с помощью эффективных политик авторизованного использования, обучения сотрудников и внедрения защиты данных в корпоративную культуру.

Обнаруживать - с полным обзором активности данных, включая растущую активность, происходящую удаленно, вне сети и в облаке.

Разрывать - благодаря способности действовать в соответствии с этой всеобъемлющей видимостью в режиме, близком к реальному времени, прерывая «слишком рискованные» действия до того, как они нанесут реальный ущерб.

Но это тоже не управление производительностью

Когда речь идёт о мониторинге всей деятельности, на ум приходят инструменты управления производительностью, которые нацелены на отслеживание всей активности пользователей и преобразование этой видимости в объективные показатели эффективности сотрудников. Но важно понимать, что решения IRM должны отличаться от управления производительностью. В конце концов, службы безопасности не заинтересованы в оценке производительности или производительности - это сфера HR. Более того, весь смысл IRM заключается в том, чтобы дать пользователям возможность работать так, как они хотят, - в развитии их изобретательности. Размывание границ в управлении эффективностью ведет IRM к определению «правильных» способов работы и, в конечном итоге, к ограничению, а не освобождению ваших сотрудников.

IRM должна быть отдельной программой, которая должна быть прозрачной и невидимой для ваших сотрудников. Прозрачный в том смысле, что ваши сотрудники полностью осведомлены о том, что и почему вы отслеживаете их деятельность, - что вам все равно, что они делают, если это не подвергает данные риску. И незаметен в том смысле, что он не замедляет работу пользователей и не снижает их продуктивность и изобретательность.

Все дело в контексте

Это простая поговорка, имеющая широкое значение: в жизни, в бизнесе - и все чаще в сфере безопасности данных - все зависит от контекста. Контекст - это ключ к расширению возможностей сотрудников работать более быстрыми и гибкими способами, защищая при этом бизнес и его наиболее конфиденциальные и ценные данные. Ясно, что обычные инструменты защиты данных, на которые полагается большинство компаний, просто не помогут в этом новом мире работы - потому что они не видят и не понимают нюансов контекста. Таким образом, так же, как компании быстро перешли к поддержке скорости и маневренности персонала, защита этой скорости и маневренности в 2021 году и далее потребует наделения групп безопасности интеллектуальной видимости быстрой и гибкой деятельности всех своих сотрудников - как в VPN, так и за ее пределами, в облаке. и в сети…». ***(A New Paradigm in Data Security: Insider Risk Management // Threatpost (https://threatpost.com/a-new-paradigm-in-data-security-insider-risk-management/164768/). 17.03.2021).***

***

«Хакерские инструменты, разработанные частными компаниями, часто используются для отслеживания и задержания диссидентов, журналистов, или политиков

За последние несколько лет сообщество специалистов по кибербезопасности неоднократно выражало тревогу по поводу постоянно растущего числа частных компаний, продающих наступательные киберинструменты (offensive cyber capabilities, OCC) иностранным правительствам без особого надзора.

Хакерские инструменты, разработанные частными компаниями, часто попадают в руки недобросовестных правительств, которые затем используют ПО для отслеживания и задержания диссидентов, журналистов, или политических соперников.

Американский аналитический центр Atlantic Council опубликовал отчет о рынке OCC и компаниях, работающих по модели «доступ-как-услуга» (Access-as-a-Service, AaaS) и продающих данные услуги. В отчете представлен анализ трех поставщиков AaaS — израильская компания NSO Group и компания DarkMatter, расположенная в ОАЭ.

В частности, эксперты рассказали об организациях, стоящих за кибератаками, в которых использовалась уязвимость нулевого дня. Из 129 атак с использованием 0Day-уязвимостей с 2014 года, 72 из них были связаны с конкретным злоумышленником. Из этих 72 случаев 14 быть связаны с частными компаниями как создателями эксплоита для уязвимости нулевого дня, использованного при атаке. Таким образом, частные компании оказались более крупным поставщиком «нулевых дней», эксплуатируемых в реальных атаках, чем правительственные и киберпреступные хакеры вместе взятые.

По словам экспертов, многие из поставщиков AaaS едва ли можно отличить от легитимных компаний, занимающихся кибербезопасностью и предоставляющих защитных решений. Данная бизнес-модель в настоящее время становится все более распространенной и текущие политики, ограничивающие экспорт и передачу инструментов OCC за границу, становятся менее эффективными, поскольку поставщики AaaS находят новые способы их обхода.

Исследователи призвали к реализации новых и улучшенных политик в отношении рынка AaaS и предложили расширить спектр уязвимостей, обнаруженных правительственными спецслужбами, о которых необходимо сообщать поставщикам, установить ограничения по окончании трудовой деятельности для государственных ИБ-сотрудников, чтобы они не могли перейти к поставщикам услуг AaaS, прибегать к практике судебных исков в отношении поставщиков AaaS и их подрядчиков, нарушающих экспортный контроль и принудить их к применению «технических ограничений», таких как географическая зона, к вредоносным программам, чтобы инструменты OCC нельзя было использовать в определенных областях или против определенных целей». ***(Большинство эксплоитов для 0Day-уязвимостей разработано частными компаниями // SecurityLab.ru (https://www.securitylab.ru/news/517152.php). 04.03.2021).***

***

«Кибератаки представляют серьезную угрозу для корпораций в целом, и те, кто занимается судоходством, не исключение. Команда Cyber Risk в Clyde & Co проработала более 3000 случаев утечки данных и киберинцидентов, включая ряд самых крупных и громких инцидентов во всем мире на сегодняшний день. Хотя эти случаи и инциденты охватили весь спектр глобальных деловых интересов, Clyde & Co имеет особенно хорошие возможности для понимания и оказания помощи в связи с резко возрастающими рисками киберпреступности, которые представляют для судоходной отрасли.

Это первая из четырех статей, в которых будут рассмотрены некоторые ключевые вопросы, связанные с угрозами, создаваемыми судоходной отраслью, и выделены некоторые из наиболее важных шагов, которые можно предпринять для снижения этого риска. В этой первой статье будут рассмотрены примеры рисков и уязвимостей, которые особенно влияют на судоходную отрасль, а также подчеркнута важность реакции на изменения в знаниях рынка посредством ссылки на претензии по договору перевозки.

Инциденты в судоходной отрасли

Большинство людей уже знакомы с кибератакой вредоносного ПО NotPetya на Maersk Line в 2017 году, которая, как сообщается, нанесла компании убытки в размере около 300 миллионов долларов США. За этим инцидентом в 2018 году последовала серьезная атака программ-вымогателей на COSCO, которая серьезно повлияла на ее электронную почту и телефонные системы в США, а также в других местах и которая, по словам компании, вызвала «существенное прерывание бизнеса». Более свежие дела, затрагивающие судоходную отрасль, включают следующее:

В апреле 2020 года компания Mediterranean Shipping Co столкнулась с атакой вредоносного ПО, в результате чего веб-сайт и штаб-квартира оператора были закрыты почти на неделю.

В сентябре 2020 года CMA CGM SA стала жертвой атаки с использованием программ-вымогателей, которая затронула некоторые серверы в ее сети и не позволила клиентам получить внешний доступ к ИТ-приложениям и системам бронирования компании.

В октябре 2020 года Международная морская организация пострадала от киберинцидента с ее ИТ-системами внутри и снаружи.

Уязвимости отрасли

Хотя судоходная отрасль в целом сталкивается с такими же киберрисками, что и другие секторы, становится все более очевидным, что она соответствует профилю особо важных объектов инфраструктуры, к которым стремятся киберпреступники, а также сталкивается с рисками, которые можно считать уникальными для природы морские перевозки грузов, например:

Системы, влияющие на навигацию судна, такие как ECDIS или AIS, могут быть атакованы для содействия пиратским, преступным или террористическим целям. Например, кибер-злоумышленник может отключить AIS судна и / или создать ложные или вводящие в заблуждение отчеты AIS. Технология, необходимая для «обмана» судна, стоит недорого, и ее становится все проще найти

и загрузить в Интернете. Инциденты со спуфингом уже наблюдались на практике в прибрежных районах России, Китая и других стран.

Все более широкое использование береговых систем управления для контроля и управления судовыми операциями предоставляет новые средства вмешательства третьих сторон или внутренних ошибок, которые могут повлиять на преследование рейса. Мы видели случаи, связанные с объектами судоходной отрасли, когда большое количество грузовых партий было неправильно направлено и / или контрактный рейс был прерван и / или серьезно задержан. Это привело к предъявлению претензий, в том числе о физической потере и / или повреждении скоропортящихся товаров и косвенных убытках.

Электронное управление грузовой документацией или системами обработки. Известно, что пираты используют кибератаки как форму разведки для определения судовых деклараций, идентификационных номеров контейнеров и морских маршрутов судов, чтобы помочь в организации атак и нацеливании на ценные товары.

По мере того, как становится очевидным возрастающий характер и масштабы угрозы, создаваемой киберпреступностью для судоходной отрасли, внимание также было сосредоточено на некоторых юридических вопросах и трудностях, связанных с такими угрозами.

Вопросы договора перевозки

В каждом случае, связанном с киберпреступностью, существует вероятность возникновения судебных исков с участием широкого круга сторон, включая судовладельцев, фрахтователей и грузовладельцев. Готовность систем судовладельца и судна к противодействию соответствующей кибератаке, вероятно, будет важным фактором в контексте таких требований.

Претензии по чартерным операциям после кибератаки могут возникнуть в связи с различными положениями, такими как те, которые касаются доставки / повторной доставки судна, лайканов, преследования рейса, задержек с погрузкой и разгрузкой, а также оплаты аренды.

В качестве конкретного примера, относящегося к договорам перевозки, большинство таких договоров будут регулироваться Гаагскими и / или Гаагско-Висбийскими правилами («Правила»), а основным обязательством перевозчика в соответствии с правилом 2 статьи III Правил является правильно и бережно хранить, перевозить и ухаживать за грузом, в том числе доставить его в договорное место без необоснованных задержек. Обязанности перевозчика в соответствии с правилом 2 статьи III подлежат исключениям, указанным в правиле 2 статьи IV. В случае кибератаки, приводящей к задержке и / или повреждению груза, перевозчики стремились использовать исключение в правиле статьи IV. 2 (q); «Любая другая причина, возникающая без фактической вины или участия перевозчика, либо без вины или небрежности агентов или служащих перевозчика…»

Однако исключения из статьи IV Правил не применяются, если перевозчик нарушает свое обязательство в соответствии с Правилом 1 статьи III Правил (обязательство по мореходности), и это очень хороший пример области, в которой, вероятно, возникнут судебные баталии. будут бороться в случаях кибератак в

будущем. Пример мореходных качеств также поучительно рассмотреть, поскольку он хорошо иллюстрирует необходимость для отрасли уделять пристальное внимание быстро меняющейся среде киберпреступности.

Мореходность

Обязанность перевозчика - проявить должную осмотрительность до и в начале рейса, чтобы предоставить мореходное судно. «Мореходность» охватывает не только физическое состояние судна, но также адекватность и эффективность экипажа, запасов и оборудования, а также пригодность судна для перевозки согласованного груза. Очевидно, что это обязательство может распространиться на убытки, возникшие в связи с киберпреступностью или атаками, но до какой степени? Как следует оценивать ответственность судовладельца в связи с этой новой и развивающейся причиной убытков?

Тест на мореходность определяется следующим образом:

«Если бы дефект существовал, необходимо задать вопрос: «Требовал бы разумный владелец, чтобы он был исправлен, прежде чем отправлять свой корабль в море, если бы он знал о нем? Если бы он захотел, корабль был бы непригоден для плавания...» (McFadden -v- Blue Star (1905) 1 KB at 706).

Так как же применить эту формулу к угрозе, исходящей от кибератак? Очевидно, что критерий «благоразумия судовладельца» предполагает, что мореходные качества следует оценивать в соответствии с уровнем знаний в отрасли на тот момент. Там, где знания и опыт в судоходной отрасли в отношении кибератак находятся на такой ранней и развивающейся стадии, шаги, которые, как ожидается, будут предприняты «благоразумным судовладельцем», в настоящее время будут подвержены высокой степени неопределенности. Это неизбежно приведет к большему количеству споров и судебных разбирательств. Совершенно ясно то, что в настоящее время на судовладельцев возлагается все возрастающее обязательство - фактически быстро растущее обязательство - избегать и снижать риск кибератак, а также обучать и обучать экипаж и другой соответствующий персонал.

Осведомленность о рынке

Признавая неотложную необходимость повышения осведомленности об угрозах киберрисков для поддержки безопасного и надежного судоходства, Резолюция ИМО MSC.428 (98) предусматривает, что вопросы киберрисков должны решаться в соответствии с Кодексом ISM и включены в системы управления безопасностью не позднее первая ежегодная проверка Документа о соответствии компании после 1 января 2021 года.

Чтобы заполнить существующие пробелы в отраслевых знаниях и помочь судовладельцам решить эту проблему, ряд отраслевых организаций собрались вместе, чтобы разработать набор руководящих принципов передовой практики. Примеры включают:

«Руководство по кибербезопасности на борту судов» (разработанное и поддерживаемое BIMCO, Международной палатой судоходства, IUMI, Intercargo, Intertanko и другими ведущими отраслевыми организациями) призвано помочь судоходным компаниям с их бортовой кибербезопасностью, предоставляя пошаговые инструкции пошаговое руководство по оценке рисков.

Лаборатория науки и технологий Министерства транспорта и обороны Великобритании разработала «Свод правил - кибербезопасность судов».

Хотя эти и другие подобные меры государственного вмешательства служат ценным и долгожданным руководством для лиц, ответственных за кибербезопасность в морском секторе, это также тот случай, когда за счет повышения общего уровня знаний в отрасли о создаваемых угрозах и профилактических мерах, которые могут быть приняты. взятые, они также могут рассматриваться как повышающие уровень обязательств, которые должны быть выполнены, чтобы соответствовать критерию «благоразумия судовладельца» в контексте иска о непригодности к плаванию. Таким образом, проблема непригодности для плавания на море служит полезной иллюстрацией повышенного уровня осведомленности и готовности, которые потребуются для решения проблемы, создаваемой киберпреступностью перед судоходной отраслью.

Конечно, помимо примера непригодности для плавания по договорам перевозки, существует множество дополнительных рисков, связанных с киберпреступностью для судоходной отрасли. В следующих статьях этой серии будет рассмотрен быстрый рост числа инцидентов с программами-вымогателями, а также вопросы, связанные с кражей и защитой данных. Мы также рассмотрим шаги, которые можно предпринять сейчас для прогнозирования и снижения рисков, включая вопросы, связанные со страхованием, и способы реагирования в случае возникновения инцидента». ***(Rosehana Amin, Rory Duncan, Daniel Jones. A very modern form of piracy: cybercrime against the shipping industry - Part 1: Rapidly developing risks // Clyde & Co LLP (https://www.clydeco.com/en/insights/2021/03/a-very-modern-form-of-piracy-cybercrime-against-th). 23.03.2021).***

***

«17 декабря 2020 года Международная ассоциация адвокатов (IBA) утвердила пересмотренные Правила IBA о получении доказательств в международном арбитраже («Правила IBA 2020»), окончательно опубликованные 17 февраля 2021 года. вопросы, связанные с удаленными слушаниями, кибербезопасностью, доцентом, заявлениями свидетелей и экспертными заключениями, назначением экспертов, перекрестным допросом или допустимостью доказательств.

Основная цель этого пересмотра заключалась в том, чтобы (i) прояснить и уточнить некоторые положения, вызывающие сомнения в отношении проведения разбирательства; (ii) включать меры предотвращения кибербезопасности и защиты данных; (iii) разрешить исключение доказательств, полученных незаконным путем, и (iv) привести Правила IBA в соответствие с новым сценарием, возникшим после COVID-19, в котором удаленные слушания с большим успехом заменили личные слушания.

Эти ключевые обновления анализируются ниже:

1. Удаленные слушания. Правила IBA 2020 включают определение «дистанционного слушания», а в статье 8 (2) отмечают необходимость разработки протокола, если стороны решат провести дистанционное слушание. Этот протокол может касаться технологии, которая будет использоваться в слушаниях,

предварительного тестирования выбранной технологии, времени начала и окончания слушаний, того, как документы могут быть размещены во время слушаний, или мер, которые должны быть приняты, чтобы гарантировать, что свидетели не будут подвержены влиянию во время слушаний.

В этом разделе к Правилам IBA 2020 добавлена практика, навязанная COVID-19, которая дает такие преимущества, как экономия времени и средств или отсутствие необходимости путешествовать, когда свидетели, арбитры и юристы находятся в разных странах.

2. Кибербезопасность. Статья 2 Правил IBA 2020 включает кибербезопасность и защиту данных среди вопросов доказывания, которые стороны обсуждают с арбитражным судом в начале разбирательства.

Мы наблюдаем все более жесткие ограничения на раскрытие конфиденциальных данных компаний и частных лиц. Добавление этой буквы e) к статье 2 Правил IBA 2020 предназначено для принятия мер по предотвращению раскрытия защищенных данных в ходе арбитражного разбирательства, а также для введения протоколов безопасности, которые уменьшают вероятность того, что третьи стороны за пределами арбитражное разбирательство с целью получения доступа к конфиденциальным данным при кибератаках.

3. Изготовление документов. Статья 3 Правил IBA 2020 прямо разрешает стороне, запрашивающей представление документов, отвечать на возражения против этого запроса, представленные другой стороной, что является широко распространенной практикой в международном арбитраже. Кроме того, дается ряд разъяснений по вопросам производства документов, в том числе различие в буквах (d) и (e) статьи 3.12, поясняющих, что документы, представленные одной стороной в ответ на запрос другой, не должны переводиться; в то время как документы, представленные в арбитражный суд, должны сопровождаться переводами на язык арбитража.

4. Показания свидетелей и заключения экспертов. Статьи 4 и 5 вносят поправку, касающуюся заявлений свидетелей и экспертных заключений, которая позволяет сторонам представлять во втором раунде представлений новые свидетельские показания или заключения экспертов в ответ на факты или вопросы, которые не были известны, когда были сделаны первые заявления или заключения. Отправлено.

5. Назначение экспертов. Поправка к статье 6 об экспертах, назначенных трибуналом, удалила следующее предложение: «Полномочия эксперта, назначенного трибуналом, запрашивать такую информацию или доступ должны быть такими же, как и у состава арбитража» . Целевая группа пришла к выводу, что этот авторитет может быть неверно истолкован как предполагающий, что назначенный судом эксперт может также разрешать любые споры относительно характера информации или доступа к ней, которые должны решаться арбитражным судом.

6. Перекрестный допрос. Статья 8, помимо предоставления полномочий составлять протокол, если слушания проводятся дистанционно, вводит в разделе 5 полномочия арбитражного суда разрешать перекрестный допрос, даже если

противная сторона прямо не требует этого. Это проясняет сомнения, которые возникли, когда другая сторона не потребовала перекрестного допроса свидетеля.

7. Допустимость доказательств. Наконец, в статье 9 Правил IBA 2020 в разделе 3 добавлены полномочия арбитражного суда по собственной инициативе или по просьбе стороны исключать доказательства, полученные незаконным путем, из разбирательства. Хотя это может показаться очевидным ограничением, факт заключается в том, что доказательства могли быть получены незаконным путем в соответствии с законодательством одной страны (например, запись без разрешения) и законно в соответствии с законодательством другой страны. По этой причине Правила IBA 2020 наделяют арбитражный суд полномочиями принимать решение о допустимости этих доказательств.

Контекст

Это третья версия Правил IBA после первого набора Правил, принятых 1 июня 1999 г., и их более поздней редакции 29 мая 2010 г. В июне 2015 г. Комитет IBA провел всемирный опрос, чтобы определить степень принятия Правила МАЮ о получении доказательств, а также другие руководящие принципы и правила, разработанные учреждением. Результаты проанализированы в Отчете о приеме продуктов IBA в области мягкого права арбитража, опубликованного в 2016 году, в котором отмечалось, что правила 2010 года часто использовались международным арбитражным сообществом, хотя некоторые положения нуждались в уточнении, чтобы улучшить их использование и признание. Поэтому была создана целевая группа, отвечающая за пересмотр Правил IBA 2010, в результате чего 17 декабря 2020 года были утверждены Правила IBA 2020.

Правила IBA 2020 будут применяться, если не согласовано иное, если стороны договорились о их применении после 17 декабря 2020 года, независимо от того, началось ли арбитражное разбирательство ранее». ***(Álvaro Soriano. New IBA rules on 2020 international arbitration: updates concerning remote hearings, cybersecurity, expert reports or witness statements // Garrigues (https://www.garrigues.com/en_GB/new/new-iba-rules-2020-international-arbitration-updates-concerning-remote-hearings-cybersecurity). 24.03.2021).***

***

«Облачная кибербезопасность - или ее отсутствие - подпитывает безумие компании, выходящие из общедоступного облака. Аналогичная озабоченность по поводу управления обязательствами по соблюдению требований удерживает организации от перехода в облако в целом.

Однако большая часть растущей озабоченности по поводу кибербезопасности облачных вычислений связана с опытом работы с публичными и частными облачными платформами. По мнению исследователей кибербезопасности, тенденция к гибридным облачным вычислениям может быть подходом к лучшему обеспечению безопасности данных.

В нескольких отчетах о кибербезопасности высказываются опасения по поводу уверенности в способности поставщиков облачных услуг адекватно защищать пользователей от утечки данных, поддерживать прозрачность и средства контроля безопасности. В отчетах возникают вопросы о решении использовать

общедоступные или частные облачные платформы или перейти к использованию гибридного облака в дополнение к существующим локальным центрам обработки данных.

Отчет, опубликованный Accurics в конце февраля, показывает, что компаниям требуется в среднем 25 дней, чтобы исправить неправильную конфигурацию облачной инфраструктуры.

Этот отчет также показывает, что 10 процентов предприятий платят за расширенные возможности облачной безопасности, которые никогда не включаются, в то время как 35 процентов организаций борются с неправильным использованием ролевого контроля доступа в облаке, что приводит к ролям со слишком большим количеством разрешений.

Результаты также показывают, что почти четверть всех нарушений связаны с плохо настроенными предложениями услуг управляемой инфраструктуры. Это упрощает злоумышленникам обнаружение служб организации, чтение их данных и, возможно, внесение изменений. Теперь атаки wateringhole возникают в облаке, где они могут нанести гораздо больший ущерб, чем в локальной среде.

Повышенный риск удаленной работы

Многие компании уже начали свои цифровые преобразования в преддверии пандемии. Между тем, британский отчет NTT о гибридном облаке показал, что Covid-19 ускорил переход к облачным хранилищам и удаленным вычислениям. Он выявил явные недостатки в возможностях облачной инфраструктуры, безопасности и сетевой архитектуры.

Сегодня существует масса проблем, связанных с защитой от кибербезопасности. По словам Дов Лернера, руководителя исследования безопасности в Cybersixgill, меры безопасности стали повышенным приоритетом благодаря Covid-19.

«Немедленный переход к удаленной работе во всем мире увеличил риск кибер-уязвимости, поскольку люди начали использовать домашние сети для работы. Поверхность угроз типичной организации значительно расширилась, поэтому надежная и сложная программа кибербезопасности имеет решающее значение», - сказал он TechNewsWorld.

Злоумышленники могут немедленно извлечь выгоду из этих новых уязвимостей, созданных удаленной работой. Используя форумы Dark Web и платформы обмена сообщениями, они могут координировать свои действия для обмена инструментами, услугами и опытом. Он добавил, что все они позволяют проводить более быстрые и изощренные атаки.

Облачная безопасность Иногда туманно

Кибербезопасность - ключевое соображение для руководителей бизнеса. Согласно исследованию NTT, в девяти из десяти решений о миграции в облако к процессу принятия решений в облаке вовлечена команда по информационной безопасности / кибербезопасности.

Компания опросила 950 лиц, принимающих решения, в 13 странах в пяти регионах. Этот отчет показал, что 61% ответивших компаний считают, что безопасность и соответствие требованиям имеют решающее значение и являются первоочередной задачей при планировании гибридного облака.

Другие результаты исследования показывают, что существует недостаток прозрачности и контроля. За последние 12 месяцев одна треть организаций перенесла приложения или данные из общедоступного облака в частные или не облачные среды. Почти треть обвиняет нарушения безопасности в качестве основного фактора перехода от общедоступного облака к частному или не облачной среде.

По мнению Майкла Ритчкена, главного консультанта NTT, устранение недостатков облачной безопасности, отмеченных в отчетах, может быть в большей степени увязано с улучшением практики внедрения облачных технологий. На самом деле, он назвал бы их не столько недостатками, сколько проблемами усыновления.

«Принятие любой новой технологии, такой как гибридные облачные платформы, сопряжено с трудностями, которые необходимо преодолеть, такими как знания, люди, процессы и инструменты», - сказал он TechNewsWorld.

Отчет NTT также показал, что производительность сети и нехватка навыков также рассматривались как значительные препятствия на пути внедрения гибридного облака. И то, и другое, если не уделить должное внимание при внедрении облака, может свести на нет те преимущества, которые оно предлагает.

Важные выводы

В отчете NTT основное внимание уделяется преимуществам внедрения гибридного облака в качестве решения общих проблемных участков облака. В отчете показаны как необходимость, так и ключевые преимущества внедрения гибридного облака по сравнению с другими вариантами хранения данных.

Как отметил Ритчкен, рынок принял как потребности, так и преимущества, и их распространение растет. Предприятия, которые еще не внедрили модель гибридной облачной платформы, планируют начать процесс внедрения в течение следующих 12 месяцев.

«Преодоление проблем управления, безопасности данных, управления и технических проблем - одни из основных проблем и препятствий, которые организации определили как препятствующие их планам по внедрению гибридных облачных платформ», - подтвердил он.

Стоимость и операционная эффективность возглавляют список внедрения гибридного облака по сравнению с другими облачными платформами. Они вызывают интерес к усыновлению.

«Я ожидаю, что внедрение гибридных облачных платформ продолжит ускоряться в ближайшие несколько лет», - прогнозирует Ритчкен.

Какая разница?

Организации могут выбирать из множества платформ облачных вычислений для доставки ИТ-приложений. Они могут предоставлять услуги клиентам или облегчать бизнес-операции. Две основные категории облачных платформ - это общедоступное облако и частное облако.

Наиболее известными общедоступными облачными платформами являются Amazon (AWS), Microsoft (Azure и O365) и Google (GCP и Google Workspace). Все вместе они называются «гипермасштабирующими облачными провайдерами» или

«гипермасштабируемыми облачными провайдерами» из-за их огромного масштаба операций.

Платформы частного облака используют аналогичные технологии с точки зрения их архитектуры и программируемости. Но они являются частными, поскольку используются одной организационной единицей, пояснил Ритчкен.

Термин гибридное облако относится к принятию нескольких облачных платформ. Они обеспечивают оптимальную доставку ИТ-приложений для получения максимальных преимуществ для бизнеса.

«При соответствующем анализе наилучшего соответствия приложений внедрение гипермасштабируемых платформ и платформ частного облака, связанных между собой для обеспечения целостной структуры инфраструктуры доставки приложений, может принести бизнесу значительные преимущества с точки зрения предоставления ИТ-приложений и услуг», - сказал он.

Еще одно существенное различие между публичными и частными облачными платформами - это потенциальная разница в доступных коммерческих моделях. Например, гипермасштабируемые платформы соответствуют финансовым моделям, основанным на потреблении, когда клиент платит за то, что он использует, на основе операционных расходов (OpEx). Платформы частного облака могут быть приобретены во многих различных коммерческих моделях, в зависимости от операционных затрат, капитальных затрат (CapEx) и гибридной коммерческой модели.

«В конечном счете, стремление к достижению оптимальной доставки ИТ-приложений и услуг со скоростью бизнеса является и будет движущей силой внедрения гибридной облачной платформы», - сказал Ритчкен.

Проблемные миграционные инициативы

До Covid-19 многие компании начали путь цифровой трансформации. Но пандемия показала, что многие облачные технологии не были такими гибкими, как раньше думали компании, использующие их. Пандемия выявила недостатки в возможностях облачной инфраструктуры, безопасности и сетевой архитектуры предприятий. Согласно исследованию, в совокупности эти проблемы препятствовали их способности адаптироваться и оставаться гибкими.

В отчете NTT говорится, что пандемия заставила предприятия полагаться на технологии больше, чем когда-либо прежде. Преимущества гибридных облаков уже очевидны. Около 61% организаций во всем мире уже используют или тестируют гибридное облако.

За гибридным облаком будущее. Исследование показало, что еще 32,7% респондентов планируют внедрить гибридное решение в течение 12–24 месяцев. Совершенно очевидно, что гибридное облако сейчас считается критически важным для процессов, управляемых данными, и принятия решений в реальном времени как сейчас, так и в будущем.

При правильной реализации гибридное облако повышает эффективность. В отчете говорится, что более эффективная совокупная стоимость ИТ-операций является основным фактором (41,3 процента) внедрения гибридного облака. Это важно, учитывая переход к модели распределенной рабочей силы, когда

предприятиям теперь необходимо получать доступ к данным и приложениям новыми, разными и часто сложными способами.

Однако предприятиям необходимо внедрить гибридное облако таким образом, чтобы оптимизировать среды для достижения максимальной эффективности. Вот почему более половины организаций (52,7%) полностью согласны с необходимостью взаимодействия с экспертами, такими как поставщики управляемых облаков.

«Чтобы преодолеть список проблем, организации обращаются к партнерам за помощью в навигации и переходе к внедрению гибридного облака», - сказал Ритчкен.

Создание лучших облаков

Одним из ключевых факторов, обнаруженных в исследовании Accurics, было то, что количество удаленных конечных точек действительно увеличивалось по всем направлениям, отметил Ом Мулчандани, технический директор, директор по информационной безопасности и соучредитель Accurics.

«Но мы также заметили, что существует множество различных облачных конечных точек, преобразованных в ботов из-за атак на конечные точки, которые также происходят в облачном пространстве», - сказал он TechNewsWorld.

Он подчеркнул, что это сочетание удаленной работы, перехода культуры на новый уровень и взломов облачных вычислений, которые позволяли злоумышленникам преобразовывать экземпляры облака в ботов». ***(Jack M. Germain. Cybersecurity Fears Trigger Migration From the Public Cloud // ECT News Network (https://www.technewsworld.com/story/87069.html). 26.03.2021).***

***

«Переход к удаленной работе в результате пандемии COVID увеличил масштаб риска и, таким образом, расширил зону ответственности менеджеров по рискам. В дополнение к соблюдению нормативных требований, количество которых продолжает расти, риск исходит из большего числа источников, чем когда-либо прежде. Среда работы из дома (WFH) предлагает новые возможности для утечки данных, нарушений политик, сбоев аудита и сторонних рисков, это лишь некоторые ИТ-риски, возникающие из-за удаленной рабочей силы.

Эта среда с высоким уровнем риска является сложной задачей для специалистов по соблюдению нормативных требований и ИТ-специалистов, которым придется отслеживать больше областей риска в этой новой среде WFH. Кибер-злоумышленники воспользовались этой возможностью и значительно расширили свои кампании в то время, когда организации наиболее уязвимы. Вероятно, что частота кибератак, таких как фишинговые атаки на удаленных сотрудников и атаки на удаленную физическую инфраструктуру, вероятно, увеличится в 2021 году, поскольку удаленная работа продолжается и даже становится нормой для многих компаний.

В дополнение к увеличению угроз кибербезопасности в следующем году, вероятно, изменится среда регулирования и управления рисками, что усугубит проблемы для сотрудников по соблюдению нормативных требований, поскольку последние нормативные изменения вступают в силу:

Недавно принятый в Калифорнии Закон о правах на конфиденциальность (CPRA) расширяет права на конфиденциальность данных в Законе Калифорнии о конфиденциальности потребителей (CCPA). Вероятно, последуют и другие состояния.

Payment Card Industry (PCI) будет выдавать новую версию своей безопасности данных Standard (DSS) для кредитных и дебетовых карт в 2021 PCI DSS 4.0 обновит правила безопасности для нужд промышленности платежей, поддержка дополнительных мер безопасности, способствовать укреплению безопасности как непрерывный процесс и усовершенствовать методы проверки.

NIST 800-53 ред. 5, опубликованная в сентябре 2020 года, станет хорошим вариантом структуры конфиденциальности, поскольку организации готовятся к появлению множества различных правил конфиденциальности.

Масштабы и сложность рисков кибербезопасности и соблюдения требований будут продолжать расти, поскольку ВФГ становится полупостоянным состоянием, даже после того, как вакцины контролируют пандемию COVID-19. В результате отделам комплаенс и ИТ потребуется найти новые способы сбора и передачи данных о рисках, определения приоритетов рисков и включения входов и выходов в масштабах всей организации.

Картина бизнес-рисков в 2021 году будет более разнообразной, опасной и плодородной, чем в прошлые годы. Вызванная пандемией среда удаленной работы будет по-прежнему вызывать значительное количество ИТ-рисков, выходящих далеко за рамки того, к чему могут привыкнуть многие специалисты по комплаенсу.

ИТ-инфраструктуры для управления и передачи данных о рисках

Существует множество различных структур информационной безопасности, которые могут принять сотрудники, отвечающие за соблюдение нормативных требований, чтобы помочь согласовать технические аспекты и язык информационной безопасности с нормативными требованиями и бизнес-рисками. Принять технологическую основу для преобразования информационной безопасности в вопросы соответствия; это поможет специалистам по комплаенсу понять, измерить, отчитаться и действовать для защиты организации от повышенных рисков, связанных с окружающей средой WFH. Риски усиливаются из-за COVID, и после его исчезновения в гибридной офисной среде они будут расти.

Фреймворк NIST CSF разработан, чтобы помочь перевести ИТ-риски в бизнес-риски и риски, связанные с соблюдением нормативных требований. Упростите и укрепите соответствие и кибербезопасность вместе, решив их с помощью стратегии информационной безопасности, ориентированной на соблюдение требований.

Шаги, которые может предпринять ваша компания

1. Объедините усилия с ИТ-отделом

Прогрессивный подход, основанный на оценке рисков, требует тесного взаимодействия отделов комплаенс и ИТ. Скорее всего, комплаенс уже сопоставил требования комплаенса с процессами; Теперь пришло время сопоставить ИТ-активы с программным обеспечением и программное обеспечение с процессами,

что создаст «Розеттский камень» для преобразования показателей информационной безопасности в бизнес-риски и цели соответствия - поддающиеся количественной оценке показатели, которые они могут измерять и по которым можно составлять отчеты.

2. Управляйте тем, что важно

Не все ИТ-события, процессы и цели соответствия требуют одинаковых вложений в управление рисками. Работайте с ИТ-отделом, управлением рисками и бизнес-лидерами, чтобы понять, что является наиболее важным, где ваши усилия по управлению рисками существуют сегодня и где вам необходимо внести корректировки для правильного подхода к управлению рисками.

3. Сопоставьте риски кибербезопасности с элементами управления и операциями

Сопоставьте ИТ-процессы с бизнес-процессами и целями. Эти сопоставления могут преобразовывать результаты информационной безопасности в условия и воздействия для бизнеса и соблюдения нормативных требований. Затем определите и уточните роли ИТ и соответствия, чтобы уточнить ответственность за соответствие ИТ и другие проблемы безопасности по мере их выявления.

4. Контекстуализировать данные о рисках для поддержки всех направлений бизнеса

Имея структуру и поток информации между отделами комплаенс и ИТ, у вас есть возможность составлять отчеты и анализировать данные о кибербезопасности и эффективности. Также становится более легкой задачей сообщать о рисках в различные направления бизнеса, такие как юридические, операционные и разработки продуктов. Обратитесь к сопоставлению элементов управления, чтобы преобразовать информацию о рисках для поддержки и защиты других направлений бизнеса.

Прошедший год продемонстрировал, насколько на самом деле взаимосвязаны глобальные риски. Картина бизнес-рисков в 2021 году будет более разнообразной, опасной и плодородной, чем в прошлые годы. Вызванная пандемией среда удаленной работы будет по-прежнему создавать значительное количество рисков для информационной безопасности, выходящих далеко за пределы того, к чему могут привыкнуть многие специалисты по соблюдению требований ... и, возможно, далеко за пределы того, что мы можем себе представить.

С другой стороны, если когда-либо и был удачный год, чтобы убедить руководство и совет директоров уделять приоритетное внимание инициативам по управлению рисками, то это 2021 год». ***(Sam Abadir. Risk Management & IT Security in the Work From Home Era // NAVEX GLOBAL (https://www.navexglobal.com/blog/article/risk-management-it-security-work-from-home/). 23.03.2021).***

***

«Руководители советов директоров по-прежнему не воспринимают кибербезопасность так серьезно, как следовало бы, и это делает организации уязвимыми для кибератак, утечек данных и программ-вымогателей,

предупредил новый руководитель Национального центра кибербезопасности (NCSC).

В своем первом выступлении после того, как она возглавила британское агентство по кибербезопасности, генеральный директор Линди Кэмерон сказала, что кибербезопасность должна рассматриваться с таким же значением для генеральных директоров, как финансовая, юридическая или любая другая жизненно важная повседневная часть предприятия.

«Пейзаж кибербезопасности, который мы видим сейчас в Великобритании, отражает огромный прогресс и относительную силу, но это не та позиция, в которой мы можем успокаиваться. Кибербезопасность по-прежнему не воспринимается так серьезно, как следовало бы, и просто не встроена в совет директоров Великобритании. думает", - сказала Кэмерон во время выступления в Королевском университете в Белфасте.

«Скорость изменений не может служить оправданием - в совете директоров цифровая грамотность так же не подлежит обсуждению, как финансовая или юридическая грамотность. Наши генеральные директора должны быть так же близки к своим директорам по информационным технологиям, как их финансовый директор и главный юрисконсульт».

Недавние киберинциденты, в том числе кампания кибершпионажа с использованием SolarWinds и кибер-злоумышленники, использующие уязвимости нулевого дня в Microsoft Exchange Server, являются лишь двумя примерами того, как организации могут столкнуться с крупномасштабными кибератаками.

NCSC заявляет, что помогло обнаружить и удалить вредоносное ПО, связанное с атакой Exchange, с 2300 компьютеров на предприятиях в Великобритании. После атаки киберпреступники бросились использовать уязвимости до того, как организации успели применить критические обновления, необходимые для их защиты.

«По мере того, как наша зависимость от технологий растет, они, к сожалению, также открывают возможности для тех, кто хочет причинить нам вред в Интернете, - сказал Кэмерон, назвав программы-вымогатели серьезной проблемой кибербезопасности для бизнеса.

«Программы-вымогатели остаются серьезной - и постоянно растущей - угрозой как с точки зрения масштаба, так и серьезности. Программы-вымогатели - это не только мошенничество и кража денег или данных, какими бы серьезными они ни были. Речь идет о потере ключевых услуг и незавидном выборе для неподготовленный бизнес».

Таков масштаб проблемы программ-вымогателей, нацеленных на школы, колледжи и университеты в последние месяцы, NCSC опубликовал предупреждение об этой проблеме с советами о том, как учреждения могут защитить себя…». ***(Danny Palmer. Boards still aren't taking cybersecurity seriously, warns new NCSC boss. That means everyone is at risk // ZDNet (https://www.zdnet.com/article/boardrooms-still-arent-taking-cybersecurity-seriously-and-thats-putting-everyone-at-risk-from-attacks-warns-new-ncsc-boss/). 26.03.2021).***

***

«Acronis опубликовал результаты своего второго ежегодного опроса Cyber Protection Week, который выявил опасное несоответствие между необходимостью организации защищать свои данные и неэффективными инвестициями, которые они сделали для достижения этой цели.

Хотя в 2020 году компании закупили новые системы для обеспечения и защиты удаленных сотрудников во время пандемии COVID-19, эти вложения не окупаются. Глобальный опрос показал, что в настоящее время 80% компаний одновременно используют до 10 решений для защиты данных и кибербезопасности, однако более половины этих организаций в прошлом году пострадали от непредвиденных простоев из-за потери данных.

Результаты ежегодного опроса Acronis, в ходе которого было опрошено 4400 ИТ-пользователей и профессионалов в 22 странах на шести континентах, развеивают миф о том, что простое добавление дополнительных решений решит проблемы кибербезопасности и защиты данных. Инвестирование в большее количество решений не только не обеспечивает большей защиты, во многих случаях попытки управлять защитой в нескольких решениях создают большую сложность и меньшую прозрачность для ИТ-группы, что увеличивает риск.

«Исследование Cyber Protection Week в этом году ясно показывает, что большее количество решений не обеспечивает более надежную защиту, поскольку использование отдельных инструментов для решения отдельных типов уязвимостей является сложным, неэффективным и дорогостоящим», - сказал Сергей «SB» Белоусов, основатель и генеральный директор Acronis. «Эти результаты подтверждают нашу веру в то, что более разумным подходом является киберзащита, которая объединяет защиту данных, кибербезопасность и управление конечными точками в одном».

Пробелы в знаниях усугубляют ИТ-проблемы

Ситуация усложняется тем, что пользователи и ИТ-специалисты не осознают, какие возможности ИТ и кибербезопасности им доступны, что может привести к потере драгоценного времени, денег и безопасности.

68% ИТ-пользователей и 20% ИТ-специалистов не знали бы, были ли их данные изменены без их ведома, потому что их решение затрудняет определение такого рода взлома.

43% ИТ-пользователей не знают, останавливает ли их средство защиты от вредоносных программ угрозы нулевого дня, потому что их решение не делает эту информацию легко доступной. Легкий доступ к такой информации о кибербезопасности имеет решающее значение для обеспечения защиты данных.

Шокирующие 10% ИТ-специалистов не знают, распространяется ли на их организацию правила конфиденциальности данных. Если лица, ответственные за обеспечение конфиденциальности данных, не знают, что они виноваты, они не могут реализовать стратегии или оценить решения, необходимые для выполнения требований. Это незнание подвергает бизнес огромному риску крупных штрафов за потенциальные нарушения в 2021 году.

Для тех, кто использует несколько решений для решения своих задач в области ИТ и кибербезопасности, непрозрачность такой информации только усугубляется. Они не только должны помнить, какое решение предоставляет

конкретную точку данных, но и постоянно переключаются между консолями, чтобы найти нужные детали, что ведет к неэффективности и упускает возможность понимания.

Слабый подход людей к защите

Опрос также выявил поразительно слабый подход к защите данных среди ИТ-пользователей.

83% ИТ-пользователей в прошлом году уделяли больше времени своим устройствам, но только половина из них предприняла дополнительные меры для защиты этих устройств.

33% признают, что не обновляли свои устройства, по крайней мере, через неделю после уведомления о патче.

90% ИТ-пользователей сообщили о выполнении резервного копирования, но 73% безвозвратно потеряли данные хотя бы один раз, что говорит о том, что они не знают, как выполнять резервное копирование или восстановление должным образом.

Усилия отдельных лиц по защите своих данных отстают от угроз, что, вероятно, связано с ложными предположениями (например, с верой в то, что Microsoft 365 выполняет резервное копирование их данных) или с использованием автоматических решений…». ***(More solutions will not solve cybersecurity and data protection challenges, study reveals // BNP Media (https://www.securitymagazine.com/articles/94919-more-solutions-will-not-solve-cybersecurity-and-data-protection-challenges-study-reveals). 30.03.2021).***

***

«Согласно исследованиям, веб-приложения по-прежнему представляют собой одну из самых серьезных угроз безопасности для организаций: более 40 процентов из них активно утекают данные, что может повлиять на бизнес и их партнеров.

Более того, производство особенно уязвимо для атак через эти приложения: как выяснили исследователи, 70 процентов приложений имеют хотя бы одну серьезную уязвимость, открытую за предыдущие 12 месяцев.

Об этом говорится в отчете компании WhiteHat Security, занимающейся безопасностью приложений, «AppSec Stats Flash Volume 3», в котором показано, как возросшая распространенность приложений, которые доступны в Интернете через веб-интерфейсы, мобильные устройства и интерфейсы на основе API, увеличила поверхность атаки и таким образом, угроза безопасности для организаций и их цепочек поставок повсюду.

Исследователи обнаружили, что среди результатов отчета содержится последовательная характеристика пяти основных уязвимостей, обнаруженных в интернет-приложениях за последние три месяца. К этим недостаткам относятся: утечка информации, недостаточный срок действия сеанса, межсайтовые сценарии, недостаточная защита транспортного уровня и подмена контента.

Облачные приложения в настоящее время являются движущей силой глобальной экономики, особенно в постпандемическом мире, в котором бизнес все чаще ведется через Интернет. Однако увеличение количества веб-приложений и

данных в облаке также означает более высокий риск утечки данных: приложения становятся все более полиморфными, с доступом через веб-интерфейсы, мобильные устройства и интерфейсы на основе API. По словам исследователей, это делает безопасность приложений сложной задачей.

«Мы продолжаем обнаруживать это окно уязвимости, ключевой показатель уязвимости остается очень высоким», - сообщил Threatpost Сету Кулкарни, вице-президент по стратегии WhiteHat. «Это означает, что веб-приложения и API-интерфейсы по-прежнему имеют серьезные уязвимости, которые можно использовать в течение всего года».

Угрозы для цепочки поставок

Что происходит, когда злоумышленник атакует цепочку поставок, в последнее время стало очень очевидным благодаря продолжающемуся фиаско SolarWinds, в котором злоумышленники использовали платформу управления сетью SolarWinds Orion для заражения пользователей с помощью скрытого бэкдора под названием Sunburst (также известного как Solorigate). Это, в свою очередь, открыло путь для бокового движения к другим частям сети.

Действительно, атаки на цепочки поставок могут быть особенно разрушительными, поскольку они затрагивают подключенные системы и бизнес-приложения, которые связаны между собой больше, чем когда-либо прежде, посредством интеграции преимущественно на основе API, заметил Кулкарни.

Эта угроза усугубляется еще одним ключевым выводом отчета о том, что среднее время, затрачиваемое организацией на исправление критических уязвимостей, по-прежнему превышает 190 дней, при этом основные классы уязвимостей остаются относительно статичными, что дает злоумышленникам «простой способ» проникнуть в по его словам, в корпоративных сетях.

«Пешеходные уязвимости продолжают преследовать приложения», - пишут исследователи. «Усилия и навыки, необходимые для обнаружения и использования этих уязвимостей, довольно низки, что упрощает задачу злоумышленника».

Производство с наибольшим риском

Производственный сектор кажется особенно уязвимым для атак из-за уязвимостей в веб-приложениях, вероятно, потому, что он «традиционно никогда не был подключен к Интернету как отрасль», а затем пришлось быстро переходить на устаревшие системы и программное обеспечение, чтобы не отставать, сказал Калкарни Threatpost.

«Рост и изменение приложений, которые никогда не должны были выходить в Интернет, чтобы стать подключенными к Интернету, вероятно, привели к такому высокому риску», - сказал он.

Еще один фактор, подвергающий производство большему риску, заключается в том, что цепочки поставок в настоящее время все больше управляются программным обеспечением, а это означает, что бизнес-партнеры теперь должны открывать внутренние приложения для интеграции с партнерами по цепочке поставок. Это снова приводит к «существующим уязвимостям, которые ранее нельзя было использовать для публичного использования», - пояснил Кулкарни.

Все это говорит о том, что устранение уязвимостей, имеющихся в интернет-приложениях организации, является «немедленной и неизбежно достижимой целью

для групп разработки и безопасности», - пишут исследователи в отчете. Этот путь к повышению безопасности начинается с того, что организации принимают меры по «снижению риска взлома в производственной среде», - сказал Кулкарни Threatpost.

«Организации должны проводить инвентаризацию общедоступных приложений, непрерывно сканировать их в производственной среде и применять подход, основанный на оценке риска, для исправления производственных проблем», - сказал он. «Это первый шаг». ***(Elizabeth Montalbano. Manufacturing's Cloud Migration Opens Door to Major Cyber-Risk // Threatpost (https://threatpost.com/manufacturing-cloud-migration-cyber-risk/165028/). 25.03.2021).***

***

«Согласно исследованию, находящиеся в стрессе сотрудники в мире удаленной работы могут быть одним из основных факторов плохой кибербезопасности компаний.

Forcepoint опросила 2000 офисных работников в Германии и Великобритании, чтобы лучше понять методы кибербезопасности среди удаленных сотрудников. Среди других результатов опрос показал, что более молодые сотрудники, а также люди, ухаживающие за детьми или другими членами семьи, сообщают о большем стрессе в своей жизни, а также о более рискованном поведении ИТ по сравнению с другими демографическими группами.

Например, 67 процентов сотрудников в возрасте до 30 лет заявили, что они используют теневые ИТ (несанкционированные приложения, услуги и оборудование), чтобы облегчить им выполнение определенных задач, по сравнению с 27 процентами сотрудников старшего возраста.

Кроме того, 55 процентов более молодой группы сообщили, что делают больше ошибок при работе из дома, например, копируют письма не тем людям - для сравнения, только 17 процентов из тех, кому за 30, сообщили о таких ошибках. И почти две трети младшей группы (63 процента) заявили, что отвлечение во время работы из дома негативно влияет на принятие решений, по сравнению с 26 процентами пожилых людей.

Неясно, является ли связь между поведением в сфере безопасности и стрессом причинной, но, по данным Forcepoint, эта взаимосвязь все же резко упускается из виду.

«Различия в поведении могут частично отражать естественные возрастные тенденции в принятии риска, но уровень несоответствия между двумя группами является как постоянным, так и экстремальным», - сказала Маргарет Каннингем, главный научный сотрудник Forcepoint, в своем сообщении в четверг на сайте журнала. Выводы. «Это может указывать на то, что естественные склонности к риску усугубляются длительными периодами стресса и сложной рабочей обстановкой».

И действительно, опрос также показал, что более двух третей (70 процентов) молодых сотрудников испытывают проблемы с концентрацией внимания из-за уровня стресса, по сравнению с 29 процентами пожилых работников, а 77 процентов заявили, что они чувствуют давление, чтобы быть доступными за

пределами нормы. рабочих часов, по сравнению с менее чем половиной (46%) пожилых работников.

Более трех четвертей (78 процентов) молодых сотрудников также сообщили, что они испытывают стресс из-за конкурирующих требований в личной и профессиональной жизни, по сравнению с 40 процентами сотрудников старшего возраста.

В то же время лица, осуществляющие уход, также переоценивают поведение, связанное со стрессом, которое негативно сказывается на практике безопасности ИТ. Например, около половины (52%) заявили, что мелкие ошибки - нормальное явление в их повседневной жизни; отвлекающие факторы, влияющие на принятие решений, также затрагивают чуть более половины группы (56 процентов). И около половины (48 процентов) признают, что используют теневые ИТ.

«Мы не ожидали, что исследование так ясно покажет картину демографических различий», - сказал Каннингем. «Изоляция была тяжелым временем для всех… без дополнительной поддержки со стороны работодателей молодые люди и лица, осуществляющие уход, могли продолжать отклоняться от заранее установленных и усвоенных правил безопасности ИТ, подвергая свои компании еще большему риску безопасности».

Она добавила, что компаниям необходимо смириться с повсеместным использованием теневой ИТ, которая подвергает организации повышенному риску кибербезопасности. Но работодатели также должны оказывать лучшую эмоциональную и личную поддержку.

«Руководители должны активно помогать сотрудникам справляться с повышенными и продолжительными уровнями стресса и беспокойства, в сочетании с дополнительными перерывами», - сказала она. «Выгорание - это не только риск для отдельных сотрудников, но также влияет на устойчивость организации и потребности в управлении кадровыми ресурсами». ***(Tara Seals. Employee Lockdown Stress May Spark Cybersecurity Risk // Threatpost (https://threatpost.com/employee-lockdown-stress-cybersecurity-risk/165050/). 26.03.2021).***

***

«Google таинственным образом удалила популярное расширение браузера ClearURLs из Интернет-магазина Chrome.

ClearURLs - это надстройка браузера, сохраняющая конфиденциальность, которая автоматически удаляет элементы отслеживания из URL-адресов. По словам его разработчика, это может помочь защитить вашу конфиденциальность при работе в Интернете.

Расширение удалено из Интернет-магазина Chrome

ClearURLs - это надстройка веб-браузера, доступная как для Google Chrome, так и для Mozilla Firefox, задача которой состоит в удалении битов отслеживания из URL-адресов.

Многие веб-сайты имеют излишне длинные URL-адреса с дополнительными параметрами, которые не имеют функциональной ценности, но используются просто для отслеживания. Это может особенно относиться к ссылкам, присутствующим в информационных бюллетенях, например: https: //example.com?

utm_source = newsletter1 & utm_medium = email & utm_campaign = sale & some_other_tracking_bits = ...

Интересно, что URL-адреса результатов поиска Google ничем не отличаются.

Например, при нажатии на результат поиска изображений Google не сразу отправляет вас на исходный URL-адрес своей веб-страницы, а скорее на промежуточный URL-адрес, который перенаправляет вас.

https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.bleepingcomputer.com%2F&psig=A XXXXX YAWa& ust = 1616XXXXXXX & source = images & cd = vfe & ved = 0C XXXX e-p3 XXX

Дополнительные параметры в приведенном выше URL (ved, cd и т. Д.) Просто отслеживают биты и источники перехода, используемые для аналитики.

ClearURLs предназначен для фильтрации таких параметров отслеживания из URL-адресов и повышения конфиденциальности пользователя в Интернете.

Если все ссылки будут лишены таких посторонних данных отслеживания, они будут иметь довольно минимальную длину, состоящую только из основных битов.

Однако вчера вечером Google совершил таинственный ход: пользователи увидели, как ClearURL исчезает из Интернет-магазина Chrome, а его страница выдавала сообщение об ошибке 404 (не найдено).

«Да, ClearURL были заблокированы Google 7 часов назад».

«Причины этого смехотворны и, вероятно, только притворяются, потому что ClearURL наносит ущерб бизнес-модели Google».

«ClearURLs выполнил свою миссию по предотвращению отслеживания по URL-адресам, и именно на этом Google зарабатывает деньги. Я думаю, что у ClearURLs сейчас так много пользователей, что это нежелательно для Google, и они хотели бы, чтобы аддон исчез навсегда», - сказал Кевин Роберт., разработчик ClearURLs.

Разработчик обратился в Google против блокировки расширения и получил известие от Google.

В копии электронного письма, предоставленного разработчиком, Google утверждает, что описание расширения «слишком подробное» и нарушает правила Интернет-магазина Chrome.

«Упоминание всех людей, которые помогали разрабатывать и переводить ClearURL, противоречит правилам Google, потому что может «запутать» пользователя. Нелепо, - продолжил Роберт.

Google также заявил, что в описании расширения не упоминаются некоторые функции, такие как функция импорта / экспорта настроек, функция ведения журнала и кнопка пожертвования, что вводит в заблуждение.

Google также заявил в письме, что расширение без необходимости требует разрешения на запись в буфер обмена.

«Но это неправда, и у меня уже более года есть описание каждого разрешения на панели инструментов разработчика Интернет-магазина Chrome».

Роберт изначально опроверг утверждение Google, заявив, что у clipboardWrite есть законная потребность в приложении для записи чистых ссылок через контекстное меню в буфер обмена.

Однако, когда его попросили дать дополнительные разъяснения по этому поводу, Роберт поделился некоторыми мыслями с BleepingComputer.

«Как оказалось, в этом больше нет необходимости, начиная с нескольких версий, потому что я переключился на другой метод копирования в буфер обмена».

«Таким образом, разрешение все еще было пережитком более ранней версии ClearURLs», - сказал Роберт BleepingComputer в интервью по электронной почте.

Но разработчик также заявил, что некоторые предложения, сделанные Google в их ответе по электронной почте, были противоречивыми.

«Описание ClearURL считается вводящим в заблуждение, потому что оно слишком подробное и описывает нерелевантные вещи».

«Что именно не имеет отношения к описанию, мне не сообщили в Google. Поэтому мне трудно это исправить».

Интересно, что это предложение Google противоречит другому предложению в том же электронном письме разработчику, где в описании функций отсутствуют подробности.

«Здесь Google говорит, что описание функций аддона недостаточно подробное и поэтому вводит пользователя в заблуждение».

Роберт имеет в виду вышеупомянутые функции: «Пожертвовать, значки, ведение журнала, экспорт / импорт».

«Это почти похоже на шутку. Ни один пользователь во время установки всерьез не заботится о том, есть ли способ сделать пожертвование, значок со значком, журнал для отладки или функция для сохранения и восстановления настроек».

«Задача аддона - очистить URL-адреса, я описал эти функции, а не то, что есть еще кнопка для пожертвований. Но Google хочет, чтобы эти «важные» функции также были описаны, потому что в противном случае пользователи «обмануты». Я добавил это к описанию», - сказал разработчик BleepingComputer.

Пользователи выражают обеспокоенность по поводу недостатков RCE в отношении "антимонопольного законодательства".

Эта разработка быстро стала появляться на публичных форумах, в том числе на сайте Y Combinator HN.

В то время как некоторые пользователи критиковали решение Google удалить расширение, ссылаясь на «антимонопольные» соображения, другие указали, что расширение ClearURLs ранее содержало ошибку выполнения произвольного кода.

Один из пользователей прокомментировал, что было довольно трудно поверить, что такая компания, как Google, была бы настолько обеспокоена этим "маленьким битым расширением", чтобы повлиять на ее бизнес-модель, или что это было основанием для удаления его из интернет-магазина. тем самым изучая утверждения разработчика расширения.

Но другие комментаторы выразили обеспокоенность тем, что огромное влияние Google на разработку Chrome, его расширений или веб-стандартов может быть проблематичным и свидетельствовать о том, что компания монополизирует эту область.

Между тем, другой комментатор утверждал, что в последний раз у расширения ClearURLs была проблема с безопасностью:

«Я бы хотел использовать ClearURL, хотя в последний раз я проверял, что у него есть серьезный недостаток: он позволяет выполнять произвольный код поставщиком списка фильтров».

«Помимо прочего, он может перенаправлять URL-адреса скриптов на произвольные источники, а список фильтров периодически обновляется со страницы GitLab, что позволяет провайдеру списка фильтров выполнять целевую атаку, обслуживая вредоносный список фильтров на определенном устройстве», но другой пользователь прокомментировал.

Многие пользователи также предположили, что этот шаг укрепил их лояльность к использованию Mozilla Firefox в качестве веб-браузера…

Пользователи Microsoft Edge также могут загрузить расширение из магазина надстроек Edge.

Роберт также выпустил более новую версию 1.21.0 с предлагаемыми обновлениями, которые, как ожидается, появятся в магазинах Mozilla и Edge в ожидании проверки». ***(Ax Sharma. Google removes privacy-focused ClearURLs Chrome extension // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/google-removes-privacy-focused-clearurls-chrome-extension/). 24.03.2021).***

***

Сполучені Штати Америки

«В новом отчете, опубликованном в четверг, Счетная палата правительства США (GAO) сообщила, что министерство обороны не сообщает четкие рекомендации по кибербезопасности подрядчикам, которым поручено создавать системы для его программ вооружений.

В рамках своих так называемых обязанностей по наблюдению за конгрессом GAO обнаружило, что программы Министерства обороны по вооружению не обеспечивают последовательного включения требований кибербезопасности в формулировки контрактов.

Например, три из пяти контрактов, рассмотренных GAO, не содержали требований к кибербезопасности, написанных на языке контрактов, когда они были заключены, с лишь расплывчатыми требованиями, добавленными позже. И из четырех родов войск только ВВС опубликовали в контрактах общеслужбы руководства по требованиям кибербезопасности.

GAO указывает, что отсутствие четких указаний по кибербезопасности проблематично, поскольку подрядчики оборонной промышленности несут ответственность только за соблюдение условий, записанных в контракте. Другими словами, если этого нет в контракте, он не будет встроен в систему.

В рамках своих рекомендаций GAO заявило, что индивидуальные требования кибербезопасности должны быть четко определены в контрактах по программам приобретения. GAO также заявило, что министерство обороны должно установить критерии для принятия или отклонения работ по контракту и того, как правительство будет проверять выполнение требований.

Министерство обороны располагает обширной сетью сложных систем вооружений, которые должны противостоять кибератакам, чтобы работать в случае необходимости. Но у Министерства обороны также есть задокументированная история поиска критически важных уязвимостей безопасности в этих программах из-за того, что, по словам GAO, недостаточно внимания к кибербезопасности систем оружия.

Отчет GAO за 2018 год показал, что DOD исторически сосредоточивал свои усилия по кибербезопасности на защите сетей и традиционных ИТ-систем. После этого отчета Министерство обороны, как сообщается, предприняло шаги, чтобы сделать свою сеть высокотехнологичных систем оружия менее уязвимой для кибератак…». ***(Natalie Gagliordi. GAO report finds DOD's weapons programs lack clear cybersecurity guidelines // ZDNet (https://www.zdnet.com/article/gao-report-finds-dods-weapons-programs-lack-clear-cybersecurity-guidelines/). 04.03.2021).***

***

«Обеспечение безопасности цепочек поставок - нелегкая задача. От разработки продукта до его окончательной поставки для одного продукта могут потребоваться сотни организаций, различные требования соответствия и широкий спектр логистических задач. Поскольку критическая инфраструктура страны зависит от информационно-коммуникационных технологий (ИКТ) для работы, сбои или нарушения безопасности в цепочке поставок ИКТ могут иметь каскадные последствия внутри и между организациями, секторами и национальными критическими функциями.

Безопасность цепочки поставок является одним из главных приоритетов Агентства по кибербезопасности и безопасности инфраструктуры (CISA) - приоритетом, которого оно достигло в значительной степени благодаря коллективным усилиям Целевой группы по управлению рисками цепочки поставок ИКТ (SCRM). Под сопредседательством Национального центра управления рисками CISA и Координационного совета по сектору информационных технологий и связи (SCC) Целевая группа представляет собой государственно-частное партнерство, объединяющее экспертов и представителей более чем сорока малых и крупных организаций для коллективного управления поставками. цепные риски.

В январе 2021 года было подписано продление на шесть месяцев устава Целевой группы, что позволит Целевой группе продолжать запускать новые или обновленные направления усилий; начать апробировать свои продукты в сообществе ИКТ и других заинтересованных сторонах; и выстраивать отношения с международными партнерами, секторами и новыми заинтересованными сторонами. Усилия в течение следующих шести месяцев будут включать работу:

Рабочая группа по обмену информацией: поскольку уязвимости в цепочке поставок ИКТ могут затронуть всех пользователей этой технологии, организации, которые делятся или получают информацию о подозреваемых поставщиках на раннем этапе процесса приобретения, могут предотвратить сопутствующий ущерб пользователям, а также всем вовлеченным организациям. Продолжая работу Целевой группы, эта РГ сосредоточит свое внимание на предложении путей, таких

как долгосрочные изменения в политике и законодательстве, которые обеспечат защиту ответственности частного сектора, чтобы способствовать обмену информацией о подозрительных поставщиках.

Рабочая группа по малому и среднему бизнесу (SMB): SMB играют значительную роль в экономике нашей страны и находятся в центре многих отраслей, таких как производство. Однако многим малым и средним предприятиям может быть сложно институционализировать руководство федеральной цепочкой поставок из-за ограниченных финансов, ресурсов и сотрудников. Эта новая РГ привлечет сообщество малого и среднего бизнеса, чтобы понять их потребности и адаптировать продукты Целевой группы, чтобы сделать их более применимыми для малых и средних предприятий.

Рабочая группа по ускорению использования продуктов: Ускорение применимости и использования продуктов Целевой группы поможет организациям управлять воздействиями рисков цепочки поставок. Эта новая РГ будет взаимодействовать с государственными учреждениями; государственные, местные, территориальные и племенные образования; академические круги (например, центры передового опыта); а также неправительственным организациям о том, как применять продукты Целевой группы в своем бизнесе, пилотировать конкретные продукты для проверки их удобства использования и учитывать отзывы, чтобы продукты оставались полезными и предоставляли значимую информацию.

Исследовательская группа по урокам, извлеченным из недавних атак на цепочки поставок программного обеспечения: по мере того, как кибератаки становятся все более изощренными, роли главного информационного директора (CIO), главного сотрудника по информационной безопасности (CISO) и персонала ИТ или кибербезопасности становятся важными для защиты организации информация и активы. В этом исследовании будет подробно рассмотрено, как рабочая группа может помочь ИТ-директорам, директорам по информационной безопасности и другим сотрудникам службы безопасности принимать более взвешенные решения с учетом рисков при закупке или развертывании определенных продуктов ИКТ, особенно тех, которые имеют административный доступ высокого уровня в рамках всей организации.

В течение следующих нескольких месяцев Целевая группа также проактивно рассмотрит будущие мероприятия и продукты, которые могут помочь организациям и агентствам реагировать на изменения в глобальном ландшафте угроз ИКТ. Эффективное управление рисками зависит от единства усилий - единства, которое Целевая группа привносит в достижение своей цели по достижению глобальной безопасности и устойчивости цепочки поставок ИКТ». ***(TASK FORCE ESTABLISHES WAY FORWARD AFTER CHARTER EXTENSION: YEAR 2.5 // Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/blog/2021/03/04/task-force-establishes-way-forward-after-charter-extension-year-25). 04.03.2021).***

***

«Какое будущее у женщин в киберпространстве?

Поскольку мы являемся первым в стране агентством по кибербезопасности, одной из наших главных целей с самого начала было увеличение представительства женщин и мужчин любого происхождения в рабочей силе CISA.

Синди М., аналитик по кибербезопасности, объясняет: «Быть частью рабочей силы CISA означает быть частью заметной и влиятельной команды, а также лидером в области кибербезопасности и инфраструктуры. Мне нравится быть частью агентства, которое может оказать влияние, которое я хочу видеть в стране и мире».

С момента основания компании CISA в 2018 году женщины выполняли широкий спектр технических функций в агентстве, в том числе возглавляли группу, которая разработала план безопасного кибер-будущего, планирование и анализ, поддерживающие внедрение вакцины COVID-19, поддержку усилий по обеспечению безопасности на выборах., разработка рекомендаций по защите систем дорогостоящих активов (HVA) в рамках федерального правительства, а также поддержка программ внутреннего разнообразия и интеграции.

«Кибербезопасность привлекла меня как захватывающая область, в которой слились воедино мое желание постоянно учиться, мой интерес и увлечение технологиями, а также моя страсть к разнообразию и инклюзивности. Я хотела быть частью отрасли, в которой я могла бы иметь значение как в развитии технологий, так и в безопасности, и произвести революцию в этой области, привнеся диверсификацию демографических характеристик, навыков и образа жизни», - продолжила Синди.

Субъекты киберугроз происходят из разных слоев общества, поэтому мы должны поддерживать штат аналитиков, лидеров и охотников за угрозами, которые могут использовать свои уникальные взгляды и опыт для точной охоты на эти угрозы.

Кроме того, разнообразная и талантливая рабочая сила может более эффективно охватить разнообразную страну, нуждающуюся в наших важнейших ресурсах. Люди из всех слоев общества должны быть в состоянии использовать, понять и получить доступ к нашим ключевым ресурсам, как кибер - советы и предметы первой необходимости для малого бизнеса, безопасности и безопасности школы и связи в чрезвычайных ситуациях.

Агентство, основанное на разнообразном опыте и идеях, гарантирует, что CISA сможет охватить всех американцев.

Важно отметить, что мы не можем сделать это в одиночку. Вот почему мы рады быть частью большого хора организаций по всему миру, которые работают над сокращением гендерного разрыва, объединяя и поддерживая женщин в области кибербезопасности. Эти организации позволяют женщинам присоединяться к группам, посещать конференции, повышать квалификацию и исследовать новые возможности в области кибербезопасности.

Мы активно налаживаем партнерские отношения с ведущими организациями, чья миссия - поощрять больше женщин в сфере высоких технологий. Работая вместе над этой общей миссией, мы сможем быстрее реализовать нашу цель - работать с мощным центром разнообразных талантов.

Месяц женской истории должен послужить для женщин настойчивым призывом использовать свои лидерские навыки и уникальные взгляды на ролях во всех областях, особенно в тех ролях, на которых женщины исторически были недопредставлены.

Следите за CISA в LinkedIn, где мы продолжим рассказывать о женщинах в CISA и важности их вклада.

В этом марте и каждый месяц мы чествуем женщин, которые проложили путь, продолжая наращивать свою численность в CISA для будущих поколений. Наша нация зависит от этого». ***(HOW CISA IS BUILDING A FUTURE FOR WOMEN IN CYBER // Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/blog/2021/03/10/how-cisa-building-future-women-cyber). 11.03.2021).***

***

«Агентство национальной безопасности (NSA) выпустило первое видео из своей новой серии выступлений Центра сотрудничества по кибербезопасности. В ходе этих переговоров эксперты АНБ поделятся своими идеями, уроками и вкладом в свою работу в области кибербезопасности. Центр работает с правительством и отраслевыми партнерами для защиты систем национальной безопасности США, Министерства обороны (DoD) и оборонной промышленной базы (DIB).

В этом первом видео заместитель главного операционного директора Центра сотрудничества в области кибербезопасности АНБ лейтенант ВМС США Закари Даннелли сел с доктором Джозией Дикстра, техническим специалистом Центра сотрудничества в области кибербезопасности, чтобы рассказать о своем опыте совместного пилотирования Protective Domain в прошлом году. Система имен (PDNS) как услуга с Центром по борьбе с информационными преступлениями Министерства обороны США (DC3) и партнерами из оборонной промышленной базы. Кроме того, Даннелли рассказал о мотивации пилотного проекта, извлеченных уроках и идеях для тех, кто может внедрить эту технологию в будущем.

Пилот PDNS изучил более 4 миллиардов DNS-запросов к участвующим сетям и из них, пометил более 3500 вредоносных доменов и заблокировал более 13 миллионов подозрительных соединений. Используя информацию, созданную журналами PDNS, лейтенант Даннелли и его команда смогли обнаружить и устранить вредоносное ПО как в сетях компании, так и на устройствах сотрудников. Несмотря на то, что кибербезопасность имеет много уровней, PDNS зарекомендовала себя в ходе этого пилотного проекта как недорогое и масштабируемое решение, которое защитники сети могут добавить в свои инструменты.

Центр сотрудничества в области кибербезопасности расширяет и расширяет возможности NSA по предотвращению и искоренению угроз для NSS, DoD и DIB через наши отраслевые партнерства. Центр сочетает в себе идеи партнеров с данными АНБ для обнаружения действий злоумышленников, создает новые инновационные технологии для обнаружения и отслеживания злоумышленников и

смягчает угрозы посредством разработки и совместного использования руководств по смягчению последствий, чтобы информировать NSS, DoD и способность DIB предотвращать и устранять угрозы». ***(NSA Cybersecurity Collaboration Center releases first speaker series video on Protective Domain Name System (PDNS) // BNP Media (https://www.securitymagazine.com/articles/94906-nsa-cybersecurity-collaboration-center-releases-first-speaker-series-video-on-protective-domain-name-system-pdns). 29.03.2021).***

***

«Компания Transmit Security выпустила отчет «Влияние паролей на ваш бизнес» - состояние проверки подлинности клиентов, в котором представлены сведения о впечатлениях клиентов, полученные на основе опроса 600 потребителей в США. Согласно результатам отчета, организации теряют потенциальных клиентов и значительную часть доходов из-за своей зависимости от традиционных систем паролей и устаревших моделей аутентификации клиентов.

В отчете также подчеркиваются проблемы, связанные с привычкой к обмену паролями. Более 50% участников опроса признают, что они поделились паролем хотя бы к одной из своих онлайн-учетных записей с кем-то еще, а 41% говорят, что они часто делятся своими паролями. Совместное использование паролей не только представляет серьезную угрозу безопасности, но и влияет на компании по разным причинам - от суммы дохода, которую они могут получить, до их способности отслеживать использование и персонализировать услуги.

Традиционные пароли также существенно влияют на качество обслуживания клиентов. Отчет Transmit Security показал, что 55% потребителей перестали использовать веб-сайт, потому что процесс входа в систему был слишком сложным, и что 87,5% потребителей оказались заблокированными в онлайн-аккаунте после слишком большого количества неудачных попыток входа в систему. Хуже того, 92% пользователей покинут веб-сайт вместо того, чтобы восстановить или сбросить свои учетные данные для входа.

Фактически, для большинства клиентов проблемы с паролями начинаются задолго до сбоя. Данные Transmit Security показывают, что 66% пользователей покинут веб-сайт, если процесс регистрации будет слишком сложным. А 64,5% покинут сайт, если их просто попросят создать имя пользователя и логин.

«Количество потребителей, которых заблокировали в своих онлайн-аккаунтах из-за неправильного ввода пароля, ошеломляет. «Клиенты выпадают из процессов транзакций - или вообще не используют сайт - из-за чрезмерно сложных и часто подверженных ошибкам систем паролей», - говорит генеральный директор и соучредитель Transmit Security Микки Будаей. «Такое ужасное обслуживание клиентов обходится предприятиям в невообразимые суммы денег, не говоря уже о доходах, которые теряются из-за обмена паролями между потребителями. Рынок готов к переменам. Пришло время избавиться от нашей зависимости от устаревшей технологии паролей и перейти к тому месту, где пароли больше не нужны»…». ***(Passwords are bad for business, frustrating for consumers // BNP Media (https://www.securitymagazine.com/articles/94918-passwords-are-bad-for-business-frustrating-for-consumers). 30.03.2021).***

***

«В рамках своей пятилетней национальной стратегии кибербезопасности стоимостью 1,9 миллиарда фунтов стерлингов (2,65 миллиона долларов США) правительство Великобритании 9 февраля объявило о создании Совета по кибербезопасности Великобритании (Совета), нового независимого органа для поддержки возможностей карьерного роста и установления профессиональных стандартов для сектора кибербезопасности Великобритании. Официально Совет будет запущен 31 марта 2021 года…

Поддержка Советом профессионального развития в области кибербезопасности будет сосредоточена на повышении прозрачности карьерных путей и определении квалификационных рамок для этих конкретных карьерных путей. Работодатели и потенциальные сотрудники будут иметь доступ к информации, касающейся необходимых навыков и опыта для работы на различных должностях в области кибербезопасности. Это поможет соискателям работы сформировать свой образовательный путь и даст работодателям уверенность в том, что новые сотрудники обладают необходимыми знаниями и техническими знаниями для выполнения работы.

Наряду с профессиональным развитием Совет будет способствовать разнообразию профессий в области кибербезопасности и будет стремиться привлекать таланты из самых разных слоев общества. Профессиональная этика - еще один главный принцип Совета, поскольку кибербезопасность играет все более важную роль в повседневной жизни, и те, кто посвятили свою карьеру обеспечению безопасности киберпространства, также должны придерживаться самых высоких стандартов, чтобы вызывать доверие общественности. Наконец, Совет обладает уникальными возможностями для оказания помощи в выработке политики и нормативных актов в области кибербезопасности, которые подчеркивают важность его интеллектуального лидерства». ***(MIKE PIERIDES, KELLI A. BOYLE. United Kingdom Forms Cyber Security Council // Morgan, Lewis & Bockius LLP (https://www.morganlewis.com/blogs/sourcingatmorganlewis/2021/03/united-kingdom-forms-cyber-security-council). 03.03.2021).***

***

«Рада ЄС схвалила висновки щодо стратегії кібербезпеки ЄС, яка окреслює план дій для захисту компаній і пересічних громадян від новітніх кіберзагроз.

Про це повідомляє пресслужба…

Стратегію у грудні 2020 року презентувала Єврокомісія та високий представник ЄС із закордонних справ.

У висновках Рада ЄС передбачає такі кроки як створення мережі безпекових центрів на всій території блоку, які б займалися моніторингом і могли заздалегідь

помічати загрозу; визначення спільного центру з кібербезпеки, який був би основним консультаційним органом для визначення політики.

Також йдеться про продовження впровадження технології зв'язку 5G та заходи для її безпечності; прискорення провадження базових стандартів інтернет-безпеки; підтримка розвитку надійного шифрування, при цьому залишаючи інструменти для роботи правоохоронців; розширення співпраці з міжнародними партнерами у сфері кібербезпеки.

Пропонують звернути особливу увагу на попередження і протидію системним кібератакам, які можуть бути спрямовані на критичну інфраструктуру, демократичні інституції та процеси.

Серед іншого, пропонують створити при Розвідувально-ситуаційному центрі ЄС (INTCEN) спеціальну групу кіберрозвідки, яка б посилила роботу відомства у цій сфері.

"Для розвитку, впровадження та моніторингу пропозицій, окреслених у стратегії кібербезпеки, Рада звертається з проханням до Єврокомісії та високого представника розробити детальний план імплементації. Рада також буде моніторити прогрес імплементації даних висновків через план дій, який буде регулярно переглядатися й оновлюватися", - додають у повідомленні». ***(Рада ЄС підтримала стратегію кібербезпеки для блоку // Європейська правда (https://www.epravda.com.ua/news/2021/03/22/672169/). 22.03.2021).***

***

Китай

«В Citizen Lab проаналізували додаток Tik Tok з метою виявлення проблем, пов'язаних з кібербезпекою, конфіденційністю і цензурою.

За словами експертів, TikTok, ймовірно, містить не більшу загрозу для користувачів, ніж соціальна мережа Facebook. Фахівці провели аналіз як додатку TikTok, доступного за межами Китаю, так і його китайської версії - Douyin.

У Китаї розробники додатків несуть відповідальність за контент, розміщений на їх платформах, що змушує їх більш активно застосовувати цензуру відповідно до державних директив, що обмежують свободу слова.

Як показали результати дослідження, ні TikTok, ні Douyin не виявляють шкідливої поведінки. Хоча Douyin містить динамічне завантаження коду і цензуру пошуку на стороні сервера, TikTok не має подібних функцій. Обидві програми мають код, що обмежує заборонений контент. Douyin обмежує деякі політичні терміни в пошуку, але поки неясно, чи є у TikTok цензура будь- якого політичного контент. Douyin також збирає додаткову інформацію про пристрої і деякі шаблони використання, які зберігаються всередині компанії і іноді передаються іншим китайським компаніям.

"У TikTok кінцевий результат налаштування загальної бази коду, схоже, створює продукт, який в значній мірі відповідає міжнародним галузевим нормам, оскільки ми не виявили ніяких небажаних функцій, подібних до тих, що є в Douyin, а також серйозних відхилень від практики конфіденційності, безпеки і цензури, в

порівнянні з Facebook", - пояснили фахівці». ***(TikTok містить не більшу загрозу для користувачів, ніж Facebook, вважають фахівці // Информационное агентство ЦК, "Эксперт-Центр" (http://expert.org.ua/smi-i-tehnologii/2021/tiktok-mistit-ne-bilshu-zagrozu-dlya-koristuvachiv-nizh-facebook-vvazhayut). 24.03.2021).***

***

Інші країни

«Сектор высшего образования в Австралии вскоре может оказаться в роли «системы национального значения», поскольку правительство готово ввести в жизнь «расширенные рамки для повышения безопасности и устойчивости» университетов через закон 2020 года о поправках к законодательству о безопасности (критическая инфраструктура).

Группа восьми (Go8), в которую входят восемь австралийских университетов, считает, что правительство на самом деле еще не определило какие-либо критически важные инфраструктурные активы в секторе высшего образования и исследований, и, следовательно, не считает, что высшее образование и исследования должны быть включены в эту категорию. сектор критической инфраструктуры с учетом нормативных требований.

«Go8 считает, что всеобъемлющий характер законодательства, предложенного для сектора высшего образования и научных исследований, является непропорциональным по отношению к вероятной степени и степени критичности этого сектора», - говорится в сообщении в прошлом месяце.

В конце 2018 года Австралийский национальный университет (ANU) подвергся серьезной утечке данных, которая была обнаружена в мае 2019 года и обнаружена двумя неделями позже, в июне.

Хакеры получили доступ к данным за 19 лет в системе, в которой находятся кадры университета, управление финансами, администрация студентов и «корпоративные системы электронных форм».

Затем был университет RMIT в Мельбурне, который в прошлом месяце отреагировал на сообщения о том, что стал жертвой фишинг-атаки, заявив, что восстановление его систем медленно продвигается.

Хотя никаких официальных заявлений относительно того, кто виноват в взломе ANU, сделано не было, генеральный директор по безопасности Австралийской разведывательной организации (ASIO) Майк Берджесс сказал, что он знает, чего было достаточно, чтобы задуматься сенатором Джеймсом Патерсоном, председателем Объединенный парламентский комитет по разведке и безопасности (PJCIS) непринужденно.

«Я знаю, кто за этим стоит. Но я бы не стал говорить об этом публично, потому что не считаю, что это моя роль», - сказал Берджесс в четверг, выступая перед PJCIS в рамках расследования рисков национальной безопасности, влияющих на Австралию. сектор высшего образования и исследований.

Что касается RMIT, то босс ASIO оставался в неведении…

Инциденты с ANU и RMIT были в центре внимания комитета, когда он проверял представителей Министерства внутренних дел и образования. Однако Патерсон надеялся найти объяснение.

«Он был назван субъектом продвинутой угрозы, но это еще не дошло до конкретных обсуждений или уточнения страны, в которой была вовлечена эта информация, эта информация не была идентифицирована», - сказал заместитель министра внутренних дел по национальной устойчивости и кибербезопасности Марк. - сказал Аблонг.

Специфика инцидента RMIT, который Аблонг называет скорее атакой, чем отключением системы, все еще расследуется…

Обсуждения вокруг двух инцидентов безопасности использовались представителем Министерства внутренних дел для оправдания включения высшего образования и исследований в законопроект о критически важной инфраструктуре…

По словам Аблонга, сектор высшего образования не осознал того, что он не уделяет должного внимания киберрискам…». ***(Asha Barbaschow. University 'hacks' as a justification to include the sector in Critical Infrastructure Bill // ZDNet (https://www.zdnet.com/article/university-hacks-as-a-justification-to-include-the-sector-in-critical-infrastructure-bill/). 11.03.2021).***

***

«Регулирующий орган в сфере телекоммуникаций Индии приостановил развертывание национальной службы «очистки» SMS и обвинил в задержке бизнес.

Власть, известная как TRAI, представила сервис очистки для ограничения текстового спама в Индии, где пользователи мобильных телефонов могут ожидать пару нежелательных сообщений каждый день, согласно приложению Truecaller для блокировки спама.

Решение этой проблемы в Индии - это режим, который требует, чтобы отправители массовых сообщений регистрировались у операторов связи и TRAI, который управляет приложением на основе блокчейна, которое ищет неожиданные сообщения в пути и очищает их до того, как они достигнут сетей или пользователей.

TRAI сообщает, что уведомил заинтересованные стороны о приложении и его требованиях в январе 2020 года. Но вчера он приостановил сервис очистки после всего дня работы, потому что законные текстовые сообщения были заблокированы.

Наблюдающий орган заявил, что проблема возникла из-за того, что операторы связи и эмитенты SMS не оформили свои документы. Между тем, такие организации, как Государственный банк Индии, в ответ на жалобы предполагают, что в этом могут быть виноваты перевозчики.

Какова бы ни была причина, проблема затрагивает граждан неприятным образом: в основном, одноразовые коды аутентификации людей для входа в службы не проходят, блокируя людей из онлайн-банкинга и т. д.

Правительство Индии также пострадало, поскольку национальное приложение для отслеживания контактов с коронавирусом Arogya Setu требует

одноразового кода, отправленного в текстовом виде, прежде чем оно будет активировано.

Регистр понимает, что скруббер SMS является расширением приложения на базе блокчейна Azure, разработанного Tech Mahindra, которое уже было с приличным успехом развернуто для блокировки спам-вызовов.

TRAI приостановил работу приложения на семь дней. Учитывая, что TRAI продвигал регистрацию SMS-сервисов более года, а законы, лежащие в основе этого, вступили в силу в 2018 году, еще неизвестно, хватит ли дополнительной недели, чтобы решить эту проблему». ***(Simon Sharwood. India pauses blockchain-powered SMS spam-scrubber after it swallows people's one-time login codes // The Register (https://www.theregister.com/2021/03/10/india_sms_blocking_mess/). 10.03.2021).***

***

«СИНГАПУР. Согласно результатам опроса, проведенного в понедельник (22 марта), малые предприятия отстают от своих более крупных коллег в области цифровой трансформации.

Они составляют 72% опрошенных компаний, которые еще не перешли на цифровую технологию.

Согласно опросу 782 малых и средних предприятий (МСП), проведенному UOB, основными причинами их сдерживания являются высокие затраты, страх перед проблемами кибербезопасности и отсутствие необходимых цифровых навыков у сотрудников. Некоторые также обеспокоены тем, что новые системы будут несовместимы со старыми.

Опубликованное в понедельник исследование UOB SME Outlook 2021 Study проводилось с конца ноября до начала декабря среди компаний с выручкой менее 100 миллионов долларов. Цель заключалась в том, чтобы понять скорость внедрения цифровых технологий малыми и средними предприятиями в Сингапуре и понять, какая поддержка необходима.

Было обнаружено, что 41% компаний, реализовавших в прошлом году инициативы по цифровизации, зарегистрировали рост доходов. Напротив, из тех МСП, которые не были оцифрованы, только 24% увидели рост выручки.

Те, кто оцифровали весь свой бизнес или несколько сфер, сообщили о лучшем росте доходов, чем те, которые оцифровали только одну сферу, в то время как шесть из 10 МСП, которые не внедрили какие-либо цифровые инструменты, в прошлом году увидели снижение чистой выручки по сравнению с 2019 годом.

МСП, перешедшие на цифровую технологию, также более оптимистичны в отношении 2021 года: трое из пяти заявили, что ожидают роста выручки в этом году, а семь из десяти заявили, что чувствуют себя более подготовленными к восстановлению бизнеса после коронавируса.

Напротив, только три из 10 малых и средних предприятий, которые не внедрили цифровые инструменты, ожидают роста выручки в 2021 году, а четыре из 10 непрофессионалов чувствуют себя более подготовленными к восстановлению бизнеса после пандемии.

Лоуренс Ло, глава подразделения бизнес-банкинга UOB, сказал: «Цифровизация предлагает компаниям множество возможностей, от улучшения их процессов и работы с новыми клиентами до прямого и измеримого влияния на их доходы».

Исследование показало, что усилия по цифровизации помогли МСП достичь большей производительности в 2020 году. Это была бизнес-цель, которую компании указали в качестве главного приоритета на год в отдельном исследовании UOB, проведенном в конце 2019 года.

МСП в сфере бизнес-услуг, производства и инжиниринга, общественных и личных услуг, технологий, средств массовой информации, телекоммуникаций и потребительских товаров продемонстрировали самый высокий процент роста производительности и эффективности в годовом исчислении - от 42 до 49 процентов.

Помимо повышения производительности, цифровизация также помогла компаниям улучшить качество обслуживания клиентов, улучшить координацию между отделами, обеспечить удаленную работу и повысить эффективность бизнеса.

Г-н Ло сказал: «Путь к цифровизации - долгий, и мы настоятельно призываем МСП придерживаться курса, чтобы увидеть, как их усилия окупятся, когда они станут сильнее в результате пандемии». ***(Jolene Ang. High costs, cyber-security fears deter small firms from going digital, study shows // Singapore Press Holdings Ltd (https://www.straitstimes.com/business/companies-markets/high-costs-and-cybersecurity-fears-deter-small-firms-from-going-digital). 22.03.2021).***

***

Кібервійни та протидія зовнішній кібернетичній агресії

«Insikt Group, разведывательная компания Recorded Future, написала документ, в котором утверждается, что за атаками на энергосистему Индии стоит Китай.

В сообщении в блоге и официальном документе (для доступа к которому требуется регистрация) компания сообщила, что заметила заметный рост целевых атак на Индию со стороны групп, спонсируемых государством.

Фирма по кибербезопасности назвала преступников "RedEcho".

Инцидент, о котором идет речь, произошел в прошлом году во время майского пограничного противостояния между Индией и Китаем. Вредоносное ПО было внедрено в 10 организаций энергетического сектора Индии и пару операторов морских портов Индии. Атака считается вероятным источником отключения электроэнергии в Мумбаи в октябре того же года.

«Используя комбинацию упреждающего обнаружения инфраструктуры злоумышленников, анализа домена и анализа записанного будущего сетевого трафика, мы определили, что подмножество этих серверов AXIOMATICASYMPTOTE разделяет некоторые общие тактики, методы и процедуры инфраструктуры (TTP) с несколькими ранее сообщенными китайскими

штатами спонсируемые группы, в том числе APT41 и Tonto Team», - говорится в отчете Recorded Future. «AXIOMATICASYMPTOTE» - это имя, данное вредоносной инфраструктуре.

Фирма заявила, что большая часть вредоносного ПО не была активирована, и связанное с этим отключение электроэнергии было результатом подмножества полезной нагрузки. Компания Recorded Future не имела доступа к коду энергосистемы Индии для более подробного анализа. Компания по кибербезопасности заявила, что связалась с индийскими властями, которые до сих пор в основном хранят молчание по этому поводу.

Связанная с технологиями напряженность между двумя странами привела к тому, что Индия запретила более 100 китайских приложений, а также создала новые инвестиционные фонды, которые явно нацелены на привлечение крупных производителей электроники из Поднебесной в Индию.

Компания Recorded Future выдвинула гипотезу, что прошлогодние отключения электроэнергии в Мумбаи, вызвавшие массовый хаос в городской инфраструктуре - от поездов до больниц и операций финансового центра, - были «демонстрацией силы», призванной предупредить Индию о возможностях Китая…

Обновлено, чтобы добавить

После того, как эта история была опубликована, правительство Индии отрицало, что отключение было вызвано заражением вредоносным ПО: причиной отказа была «человеческая ошибка».

Министр энергетики Союза Р.К. Сингх, однако, признал, что вредоносное программное обеспечение проникло в центры распределения нагрузки северного и южного регионов Индии, хотя, как нам сказали, воздействие было ограниченным». ***(Laura Dobberstein. Malware attack that crippled Mumbai's power system came from China, claims infosec intel outfit Recorded Future // The Register (https://www.theregister.com/2021/03/01/statesponsored_chinese_group_attacked_india/). 01.03.2021).***

***

«Хакеры китайского национального государства были связаны с атакой на парламент Финляндии, которая произошла в прошлом году и привела к компрометации некоторых учетных записей электронной почты парламента.

«Некоторые учетные записи электронной почты парламента, возможно, были скомпрометированы в результате атаки, в том числе учетные записи электронной почты, принадлежащие депутатам», - заявили тогда представители парламента.

Нападение было обнаружено группой безопасности парламента Финляндии, и в настоящее время оно расследуется Национальным бюро расследований Финляндии (NBI) с помощью полиции безопасности и Центральной уголовной полиции.

«В прошлом году полиция безопасности определила состояние операции кибер-шпионаж против парламента, который пытался проникнуть в информационные системы парламента,» заявление, опубликованное сегодня читает. «По данным полиции безопасности, это была так называемая операция APT31».

Комиссар Центральной криминальной полиции Теро Муурман добавил, что дальнейшие подробности нападения не будут разглашаться, пока расследование еще продолжается…

APT31 шпионские кампании

APT31 (также известная как Zirconium и Judgment Panda) - поддерживаемая Китаем хакерская группа, известная своим участием в многочисленных операциях по краже информации и шпионажу, работающей по указанию правительства Китая.

…APT-группа также была связана с кражей и перепрофилированием эксплойта EpMe NSA за несколько лет до того, как Shadow Brokers публично раскрыли его в апреле 2017 года.

В прошлом году Microsoft зафиксировала атаки APT31 на лидеров международного сообщества и известных лиц, связанных с президентской кампанией Джо Байдена.

APT31 также был замечен Google при нацеливании на «личные электронные письма сотрудников кампании с учетными фишинговыми электронными письмами и электронные письма, содержащие ссылки для отслеживания»…». ***(Sergiu Gatlan. Chinese nation state hackers linked to Finnish Parliament hack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/chinese-nation-state-hackers-linked-to-finnish-parliament-hack/). 18.03.2021).***

***

«Розслідування кібератаки на Державну службу зайнятості Іспанії, якої вона зазнала 9 березня, вказує на те, що за атакою стоїть Росія…

Як зазначається, кібератака – це відповідь Москви на низку дипломатичних та військових інцидентів між, з одного боку, Кремлем, а з іншого - урядом та іспанськими збройними силами.

Держслужбу зайнятості Іспанії було атаковано вірусом типу ``ramsomware", який шифрує файли та блокує комп'ютери, щоб отримати викуп, як правило, в криптовалюті, в обмін на відновлення нормальної роботи. Ці кібератаки мають сенс проти компаній, які іноді платять хакерам, але не проти установ, які не можуть поступитися шантажу.

Метою кібератаки була скоріше дискредитація державної установи та держави, якій вона належить, та викликання невдоволення громадськості через скасування тисяч призначень по всій Іспанії та параліч обробки даних щодо допомоги по безробіттю, особливо під час кризи.

Іспанія, поряд з Німеччиною, є державою з певною вагою в Європейському союзі, яка за останні місяці мала найгірші відносини з Росією. У цій країні три роки тому була створена зловмисна програма Ruyk, за допомогою якої групи кіберзлочинців здійснили численні атаки, багато з яких, ймовірно, були за замовленням ФСБ Росії.

Розслідування, проведене в Іспанії Національним інститутом кібербезпеки та Національним криптологічним центром (при Національному центрі розвідки) може чітко вказати на Москву як відповідальну за кібератаку.

Якщо Німеччина вступила в конфронтацію з Росією у справі опозиціонера Алексєя Навального, то напруженість з Іспанією виникла після невдалого візиту

глави європейської дипломатії Жозепа Борреля у лютому. Після цього візиту 27 країн-членів затвердили нові санкції проти Росії 22 лютого. Уряд Іспанії брав участь у суперечці Борреля-Лаврова через міністра закордонних справ Аранчу Гонсалес Лаю. Це закінчилося нагадуванням, що Іспанія є "однією з 23 повноцінних демократій у світі", тоді як "Росія займає 124 місце з 167 країн".

Також видання згадує про інциденти з перехоплення російських винищувачів іспанськими над Чорним морем, а також присутність іспанських кораблів у Чорному морі, що дратує Росію». ***(Розвідка Іспанії підозрює РФ у кібератаці на Держслужбу зайнятості – ЗМІ // Європейська правда (https://www.eurointegration.com.ua/news/2021/03/22/7121160/). 22.03.2021).***

***

«У Німеччині хакери намагалися здійснити атаку на сімох депутатів Бундестагу й на 31 депутата місцевих парламентів.

Від атаки постраждала низка політичних активістів…

Повідомляється, що хакерської атаки зазнали переважно члени правлячих партій — Християнсько-демократичного союзу, Християнсько-соціального союзу, Соціал-демократичної партії Німеччини. На цей час не встановлено, чи стався витік даних з акаунтів депутатів.

Зазначається, що депутатів намагалися зламати за допомогою фішингового повідомлення зі шкідливими посиланнями, метою яких було захоплення всього облікового запису користувача. Інших подробиць не наводиться. Повідомляється, що за атакою може стояти угрупування Ghostwriter, яке пов’язують з Росією і ГРУ…». ***(Пов’язані з РФ хакери намагалися зламати німецьких депутатів // Ракурс (https://racurs.ua/ua/n152340-pov-yazani-z-rf-hakery-namagalysya-zlamaty-nimeckyh-deputativ.html). 26.03.2021).***

***

«Поліція Бельгії розслідує кібератаку, від якої минулого року постраждала служба прем’єр-міністра Александра де Кроо.

Про це повідомляють бельгійські ЗМІ, серед яких The Brussels Times, пише "Європейська правда".

Александр де Кроо повідомив, що у минулому 2020 році у комп’ютерній мережі його служби виявили три "специфічні інциденти, пов’язані з безпекою", після чого знадобилось втручання фахівців.

Після інцидентів запровадили додаткові заходи безпеки, а один з них розслідує поліція. Втім, серйозної шкоди мережі завдати не встигли.

"На цей час ми не маємо жодної інформації про те, хто стоїть за атакою", - зазначив Александр де Кроо.

Коли саме сталися інциденти, не уточнюють». ***(Поліція Бельгії розслідує кібератаку проти прем’єра // Європейська правда (https://www.eurointegration.com.ua/news/2021/03/4/7120505/). 04.03.2021).***

***

«В ходе того, что было объявлено крупнейшим обновлением стратегии безопасности и внешней политики со времен холодной войны, правительство Великобритании обозначило новые оборонные приоритеты, в основе которых лежит настоятельная необходимость активизировать использование новых технологий для защиты страны.

Премьер-министр Борис Джонсон на этой неделе представил комплексный обзор, который готовился более года и будет использоваться в качестве руководства для принятия решений о расходах в будущем. Сосредоточившись на внешней политике, обороне и безопасности, в обзоре поставлены цели для Великобритании до 2025 года; а в основе многих целей лежит задача модернизации вооруженных сил страны.

…правительство кажется особенно амбициозным в сфере кибербезопасности: в документе обещается приверженность новому, «полному спектру» подхода к киберпотенциалам Великобритании, чтобы лучше обнаруживать, пресекать и сдерживать злоумышленников…

Киберугроза, исходящая от иностранных государств, в прошлом неоднократно доводилась до сведения правительства. В прошлом году начальник военной разведки Великобритании Джеймс Хокенхалл предостерег от растущих проблем, создаваемых Россией и Китаем, которые, как он утверждал, усиливают традиционные методы конфликта, а также вкладывают значительные средства в кибернетику.

Примерно в то же время в отчете комитета парламентариев возможности России по кибератакам описываются как «непосредственная и неотложная угроза» национальной безопасности страны, приводятся примеры того, как российские хакеры вторгаются в критически важную инфраструктуру Великобритании и организуют попытки фишинга против правительственных ведомств.

В новом интегрированном обзоре предлагается разработать киберстратегию в конце этого года, которая позиционируется как основанная на «полностью кибернетическом» подходе, который рассматривает ряд возможностей. Помимо укрепления киберэкосистемы страны и создания более безопасного онлайн-пространства, кибер-стратегия откроет возможности для Великобритании стать лидером в технологиях, жизненно важных для кибернетической мощи, таких как микропроцессоры, квантовые технологии и новые формы передачи данных…

Примечательно, что кибер-стратегия будет сосредоточена на активном подрыве действий злоумышленников, возлагая на них издержки или лишая их возможности нанести ущерб интересам Великобритании - шаг вперед от чисто защитного подхода к кибербезопасности.

Центральным в наступательном подходе Великобритании будет официальное учреждение Национальной киберсилы (NCF), штаб-квартира которой, как объявил премьер-министр, будет размещена на севере Англии в попытке создать «кибер коридор» по всему региону. Благодаря этому промышленность и университеты на севере страны будут работать рука об руку с правительственными экспертами для предотвращения кибератак.

NCF, созданный только в прошлом году, представляет собой партнерство между Министерством обороны (MoD) и Управлением правительственной связи (GCHQ), которое привлекает сотрудников обеих организаций с экспертами из Секретной разведывательной службы (MI6) и Лаборатории оборонной науки и технологий. (DSTL). Другими словами, он впервые объединяет ключевых игроков с общей задачей - проводить целенаправленные наступательные кибероперации против террористов, враждебных государств и преступных группировок…

Вполне вероятно, что NCF фокусируется на кибероперациях, которые могут нарушить способность злоумышленника действовать, а не атаковать его в лоб. Правительство определило некоторые операции, которые могут выполнять силы, в том числе вмешательство в мобильный телефон, чтобы не дать террористам общаться со своими контактами, а также предотвращение использования киберпространства для совершения серьезных преступлений или обеспечение безопасности военных самолетов от поражения с помощью оружия.

Система

Атаки, осуществленные NCF, вероятно, примут форму, аналогичную тем, которые описаны директором GCHQ Джереми Флемингом в 2018 году, который в то время объяснил, как организация предпринимала наступательные действия в Интернете, чтобы остановить распространение пропаганды Даиш и воспрепятствовать террористам».

Способность координировать атаки

Однако, по мнению некоторых критиков, требуется дополнительная работа, чтобы убедиться, что NCF теперь занял свое место среди всех хорошо зарекомендовавших себя государственных институтов безопасности. «Приятно видеть акцент на кибербезопасности в целом с тем, что является явно наступательной киберсилой, но это больше похоже на коммерческое предложение того, что является значительным вложением ресурсов в то, что может быть непопулярным», - Эндрю Дуайер, исследователь кибербезопасности в Даремском университете, сообщает ZDNet.

«Неясно, какова на самом деле миссия NCF - похоже, что сила, которая еще не определила, что ей нужно или чего хочет. Существует вероятность того, что движение на север может придать NCF некоторую идентичность, отличную от ее основных участников - MoD и GCHQ - но, вероятно, потребуется гораздо более детальная работа, чтобы довести его до оперативной готовности», - продолжает он…». ***(Daphne Leprince-Ringuet. Cyber strength now key to national security, says UK // ZDNet (https://www.zdnet.com/article/cyber-strength-now-key-to-national-security-says-uk/). 17.03.2021).***

***

Кібератака на SolarWinds

«Компания по обеспечению безопасности электронной почты Mimecast заявила во вторник, что завершила судебно-медицинское расследование

последствий атаки на цепочку поставок SolarWinds и показала, что злоумышленнику удалось украсть некоторый исходный код.

Mimecast была одной из нескольких компаний, занимающихся кибербезопасностью, которая подтвердила, что стала целью хакеров, взломавших системы поставщика решений для управления ИТ SolarWinds.

После компрометации систем SolarWinds злоумышленники, связанные с Россией, использовали свой доступ для доставки вредоносных обновлений к продуктам мониторинга SolarWinds Orion примерно 18 000 клиентов. Несколько сотен из этих клиентов, включая государственные и частные организации, подверглись дальнейшему нападению.

Одной из таких целей был Mimecast, который узнал о вторжении от Microsoft. Технический гигант заметил, что сертификат, используемый клиентами Mimecast для аутентификации определенных продуктов с помощью служб Microsoft 365, был скомпрометирован.

Расследование, проведенное с помощью подразделения FireEye по реагированию на инциденты Mandiant, показало, что хакеры получили доступ к части производственной среды Mimecast с помощью вредоносного ПО SUNBURST, доставленного через вредоносные обновления продукта Orion.

Затем злоумышленник смог продвинуться горизонтально в скомпрометированной среде, получив доступ к различным типам систем и информации.

Скомпрометированный сертификат, обнаруженный Microsoft, был использован злоумышленниками для подключения к клиентам Microsoft 365 с «малым однозначным числом» клиентов.

Кроме того, хакеры получили зашифрованные учетные данные сервисных аккаунтов, созданные клиентами в США и Великобритании. Эти учетные данные, используемые для подключений между клиентами Mimecast и локальными и облачными службами, по всей видимости, не были расшифрованы или использованы неправильно.

«У нас нет доказательств того, что злоумышленник получил доступ к электронной почте или архивному контенту, который мы храним от имени наших клиентов», - говорится в отчете Mimecast…

Однако злоумышленникам удалось получить доступ к «подмножеству» адресов электронных почт и другой контактной информации, а также к хешированным и засекреченным учетным данным. Попавшие под удар клиенты были уведомлены.

Расследование также показало, что злоумышленники - аналогично тому, что они сделали в случае с другими жертвами, включая Microsoft - также получили доступ и загрузили «ограниченное количество» репозиториев исходного кода.

«Мы считаем, что исходный код, загруженный злоумышленниками, был неполным и недостаточным для создания и запуска любого аспекта службы Mimecast. Мы не нашли доказательств того, что злоумышленники внесли какие-либо изменения в наш исходный код, и не считаем, что это оказало какое-либо влияние на наши продукты», - сказал Mimecast.

В ответ на инцидент компания по кибербезопасности поменяла все затронутые ключи шифрования и сертификаты, прекратила использование продукта Orion, изменила все учетные данные сотрудников и системы, повысила безопасность аутентификации, полностью заменила все взломанные серверы и развернула дополнительные системы мониторинга безопасности». ***(Eduard Kovacs. Mimecast Says SolarWinds Hackers Stole Source Code // Wired Business Media (https://www.securityweek.com/mimecast-says-solarwinds-hackers-stole-source-code). 17.03.2021).***

***

«117- й Конгресс начал свою первую сессию, среди прочего, с слушаний по надзору за кибер-взломом SolarWinds. 23 февраля Комитет Сената по разведке провел слушание по громкому и далеко идущему нарушению; с последующим совместным слушанием. 26 февраля в Палате представителей, проведенных комитетами по надзору и реформам и национальной безопасности. На обоих слушаниях выступили Судхакар Рамакришна, президент и генеральный директор SolarWinds, Кевин Мандиа, генеральный директор FireEye, и Брэд Смит, президент и главный юридический директор Microsoft. Кроме того, Джордж Курц, президент и главный исполнительный директор Crowdstrike, дал показания на слушаниях в сенатской разведке, а Кевин Томпсон, бывший генеральный директор SolarWinds, дал показания перед совместными слушаниями Палаты представителей. Вместе слушания представляют собой то, что, вероятно, станет первым из нескольких набегов Конгресса на взлом SolarWinds, включая возможные законодательные инициативы по устранению возможных инцидентов в будущем и обеспечению безопасности цепочки поставок.

Фон

Напомним, SolarWinds - это компания, занимающаяся информационными технологиями (ИТ) (базирующаяся в Остине, штат Техас), которая предоставляет продукты бизнес-клиентам и федеральному правительству, позволяя им контролировать свои ИТ-сети и управлять ими. В декабре компания FireEye, занимающаяся кибербезопасностью, сообщила, что хакеры, вероятно, из России (если не самого российского правительства), использовали набор инструментов мониторинга и управления сетью SolarWinds, Orion, для распространения вредоносного ПО по ИТ-сетям клиентов SolarWinds. В частности, хакеры использовали систему обновлений Orion, которая рассылает обновления и исправления сетевого программного обеспечения, для создания векторов входа, известных как «бэкдоры», для тайного проникновения на платформы управления ИТ SolarWinds. Попав внутрь, вредоносная программа, известная как «SUNBURST», смогла эффективно выполнять новые команды и извлекать файлы, маскируя свои действия под безобидный трафик, неотличимый от других потоков данных в зараженных сетях. Так продолжалось не менее девяти месяцев до открытия FireFly.

Хотя вся совокупность лиц, пострадавших от взлома, неизвестна, по оценкам SolarWinds, 18 000 из более чем 300 000 клиентов уязвимы для этого вредоносного ПО. По оценкам New York Times, пострадало до 250 государственных учреждений

и компаний. Кроме того, остается неизвестным намерение российского взлома - была ли это шпионская кампания по сбору информации или более злонамеренная атака, направленная на причинение вреда?

…Взлом SolarWinds является последним из серии широко известных кибернетических нарушений и взломов данных, которые длились несколько десятилетий и поставили под угрозу безопасность государственных учреждений и корпоративных корпораций Америки, а также конфиденциальность миллионов американцев. За последние несколько лет Конгресс принял множество законов, направленных на улучшение позиции Америки в отношении кибератак и безопасности цепочек поставок. Такие законы, как Закон о повышении уровня кибербезопасности, Федеральный закон о монетизации информационной безопасности (FISMA), Закон об обмене информацией о кибербезопасности (CISA) и Закон об улучшении кибербезопасности Интернета вещей (IoT), устранили недостатки кибербезопасности путем кодификации Национального института стандартов и технологий (NIST), а также разработали рамки кибербезопасности, устанавливающие полномочия Министерства внутренней безопасности (DHS) над кибер-практикой федеральных агентств, обеспечивающие защиту ответственности для стимулирования обмена информацией об угрозах и разработку федеральных стандартов для использования приобретаемых на федеральном уровне устройств IoT, соответственно. Тем не менее, несмотря на эти важные законы, слушания на прошлой неделе по поводу взлома SolarWinds показали, что Конгресс готов принять дальнейшие законодательные меры.

Соображения политики

И на слушаниях в Сенате и Палате представителей члены в основном сосредоточили свои вопросы на том, что произошло, на степени ущерба и на том, как Конгресс может помочь предотвратить повторение инцидентов в будущем…

Во-первых, члены и свидетели в целом согласились с тем, что стране нужна более крупная, лучше подготовленная кибер-рабочая сила.

Во-вторых, многие участники согласились с тем, что необходимо выделить больше ресурсов на усиление киберзащиты страны, будь то дополнительные инвестиции федерального правительства или обновление устаревшего программного обеспечения и систем безопасности большей части критически важной инфраструктуры страны…

В-третьих, многие члены сосредоточили внимание на необходимости улучшения «кибергигиены» и «передовой практики», которые все чаще могут включать практику «охоты за угрозами» (охота за угрозами - это упреждающая практика постоянного поиска киберугроз в сети)… Структура NIST уже описывает лучшие практики кибербезопасности, подходящие для целого ряда заинтересованных сторон, больших и малых, и поиск угроз, вероятно, может стать частью следующей редакции Структуры (в настоящее время проходит пересмотр)…

В-четвертых, многие члены и свидетели заявили о необходимости улучшения «государственно-частного партнерства» для устранения повсеместных угроз кибербезопасности. Такое сотрудничество имеет множество политических аспектов… Фактически, в основе NIST Framework лежит государственно-частное

сотрудничество, в ходе которого были разработаны добровольные руководящие принципы безопасности, которые почти повсеместно хвалят как эффективный, практичный, гибкий и развивающийся план кибергигиены, который может быть принят заинтересованными сторонами критически важной инфраструктуры.

Более того, в рамках этого государственно-частного партнерства как члены, так и свидетели заявили о необходимости более активного обмена соответствующей информацией… Такой обмен информацией включает предоставление сведений об угрозах частным заинтересованным сторонам, находящимся в аналогичном положении, с целью максимизировать скорость и эффективность коллективного реагирования на угрозы.

Несколько раз свидетели выражали озабоченность по поводу юридической ответственности и «преследования жертв» после громких нарушений. В этой ноте (и как отмечалось выше) CISA, который Конгресс принял в 2015 году как часть комплексного пакета расходов, уже предоставляет компаниям защиту от ответственности, чтобы побудить их делиться информацией об «индикаторах киберугроз» и «защитных мерах» с федеральными властями, правительствами штатов и органами местного самоуправления, а также другими компаниями. Обмен такой информацией должен соответствовать протоколам, изложенным в CISA… Кроме того, Отчет генерального инспектора DHS за сентябрь 2020 года показал, что CISA и агентство по реализации закона, вышеупомянутое Агентство по кибербезопасности и безопасности инфраструктуры (также известное как CISA), добились прогресса в стимулировании более широкого обмена информацией благодаря участию в Автоматизированном обмене показателями (AIS)…» ***(Christian T. Fjeld. Hearings on the SolarWinds Hack and Possible Policy Responses // Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C. (https://www.mintz.com/insights-center/viewpoints/2236/2021-03-04-hearings-solarwinds-hack-and-possible-policy-responses#page=1). 04.03.2021).***

***

«Microsoft раскрыла другие вредоносные программы, которые использовались предполагаемыми хакерами, поддерживаемыми российским правительством, которые внедрили вредоносное ПО в программное обеспечение американского поставщика программного обеспечения SolarWinds.

Microsoft назвала субъектов угрозы как Nobelium, продолжая традицию называть известные хакерские группы национальных государств в честь химических элементов, таких как российский стронций, китайский барий, иранский фосфор и северокорейский таллий.

До сих пор Microsoft и поставщик средств безопасности FireEye идентифицировали вредоносные программы Sunburst (которые Microsoft называла Solorigate) и Teardrop. В январе охранная фирма CrowdStrike обнаружила Sunspot, программу, предназначенную для мониторинга сервера сборки на предмет команд сборки, которые собирают Orion.

Orion является программным обеспечением для мониторинга SolarWinds сети, Nobelium злоумышленники использовали для широко распространить

Sunburst бэкдор 18,000 организаций в течение 2020 года, до Cherrypicking девяти федеральных агентств США и около 100 американских компаний, на самом деле компромисса и украсть информацию, в соответствии с Белым домом «с изучение.

Microsoft раскрыла три новых вредоносных компонента, используемых хакерами Nobelium: GoldMax, GoldFinder и Sibot. FireEye называет группу UNC2452, назвав недавно обнаруженную вредоносную программу Sunshuttle.

GoldMax рассматривается Microsoft как имплант, служащий бэкдором управления и контроля (C2). Бэкдор был написан на популярном языке системного программирования Google, Go.

FireEye заявила, что не знает, как установлено это вредоносное ПО, но предполагает, что это второстепенный бэкдор, сброшенный после первоначального взлома. Компания охарактеризовала дизайн Sunshuttle как «изысканный» и «элегантный».

«Новый бэкдор SUNSHUTTLE - это сложный бэкдор второго уровня, который демонстрирует простые, но элегантные методы уклонения от обнаружения за счет «смешанного» трафика для связи C2», - отмечает FireEye в своем анализе.

GoldMax используется исключительно для связи с C2 злоумышленника и полагается на перепроданные домены с высокой репутацией, которые создавались с течением времени. По словам Microsoft, такой выбор доменов помог GoldMax избежать срабатывания сигналов тревоги в большинстве продуктов безопасности, которые таким образом оценивают репутацию.

«Вредоносная программа записывает зашифрованный файл конфигурации на диск, где имя файла и ключи шифрования AES-256 уникальны для каждого имплантата и основаны на переменных среды и информации о сети, в которой оно работает», - поясняет Microsoft.

«GoldMax устанавливает безопасный сеансовый ключ со своим C2 и использует этот ключ для безопасного взаимодействия с C2, предотвращая получение и идентификацию вредоносного трафика соединениями, не инициированными GoldMax».

По словам Microsoft, Sibot, созданный с помощью Microsoft Visual Basic Scripting (VBScript), представляет собой вредоносное ПО двойного назначения.

«Файлу VBScript дается имя, которое олицетворяет законные задачи Windows, и оно либо хранится в реестре скомпрометированной системы, либо в запутанном формате на диске. Затем VBScript запускается через запланированную задачу», - отмечает Microsoft.

Его основной целью было сохранение на зараженной машине, чтобы она могла загружать и выполнять полезные данные с удаленного сервера C2. Microsoft определила три варианта Sibot, каждый из которых загружает вредоносную полезную нагрузку.

GoldFinder, который также написан на Go, считается настраиваемым инструментом HTTP-трассировки, который регистрирует маршрут или переходы, которые принимает пакет, чтобы достичь жестко запрограммированного сервера C2.

В рамках более широкой хакерской кампании, поддерживаемой Россией, некоторые компании, занимающиеся кибербезопасностью, были

скомпрометированы с помощью испорченного обновления Orion SolarWinds, например, Microsoft, но это был не единственный способ проникновения хакеров в системы; 30% взломанных организаций не имели прямой связи с Solar Winds и подверглись атакам другими способами». ***(Liam Tung. Microsoft: We've found three more pieces of malware used by the SolarWinds attackers // ZDNet (https://www.zdnet.com/article/microsoft-weve-found-three-more-pieces-of-malware-used-by-the-solarwinds-attackers/). 05.03.2021).***

***

«Подозреваемые российские хакеры получили доступ к учетным записям электронной почты, принадлежащим главе Департамента внутренней безопасности администрации Трампа и сотрудникам отдела кибербезопасности, чья работа включала охоту на угрозы из зарубежных стран…

Информационная ценность взлома тогдашнего государственного секретаря Чада Вольфа и его сотрудников публично не известна, но символизм очевиден. Доступ к их учетным записям был осуществлен в рамках так называемого вторжения SolarWinds, и это ставит под вопрос, как правительство США может защитить людей, компании и учреждения по всей стране, если оно не может защитить себя.

Короткий ответ для многих экспертов по безопасности и федеральных чиновников заключается в том, что это невозможно - по крайней мере, без некоторых существенных изменений.

«Взлом SolarWinds стал победой для наших иностранных противников и провалом для DHS», - сказал сенатор Роб Портман из Огайо, главный республиканец в Комитете Сената по внутренней безопасности и делам правительства. «Мы говорим о жемчужинах DHS».

Администрация Байдена пыталась держать в секрете масштабы атаки SolarWinds, поскольку она взвешивает ответные меры против России. Но запрос AP обнаружил новые подробности взлома в DHS и других агентствах, включая Министерство энергетики, где хакеры получали доступ к расписаниям высших должностных лиц.

AP взяло интервью у более чем десятка нынешних и бывших правительственных чиновников США, которые говорили на условиях анонимности из-за конфиденциального характера продолжающегося расследования взлома.

Уязвимости в Homeland Security, в частности, усиливают беспокойство после атаки SolarWinds и еще более широкого взлома почтовой программы Microsoft Exchange, особенно потому, что в обоих случаях хакеры были обнаружены не правительством, а частной компанией.

В декабре официальные лица обнаружили то, что они описывают как разрастающуюся, продолжавшуюся несколько месяцев, кибершпионаж, в основном за счет взлома широко используемого программного обеспечения от компании SolarWinds Inc., расположенной в Техасе. По меньшей мере девять федеральных агентств были взломаны вместе с десятками компаний частного сектора.

Власти США заявили, что взлом, по всей видимости, был делом рук российских хакеров. Генерал Пол Накасоне, возглавляющий киберсилы Пентагона, заявил на прошлой неделе, что администрация Байдена рассматривает «ряд вариантов» ответа. Россия отрицает свою причастность к взлому.

С тех пор серия громких хакерских атак еще больше высветила уязвимости в государственном и частном секторах США…

Сенатор Марк Уорнер, демократ из Вирджинии и глава сенатского комитета по разведке, сказал, что первоначальная реакция правительства на обнаружение взлома SolarWinds была несвязной.

«Что меня поразило, так это то, как долго мы оставались в темноте, пока оставались в темноте», - сказал Уорнер на недавней конференции по кибербезопасности.

По словам нынешних и бывших официальных лиц, Вольф и другие высокопоставленные чиновники национальной безопасности использовали новые телефоны, которые были очищены, а также популярную систему зашифрованных сообщений Signal для связи в первые дни после взлома.

Один из бывших должностных лиц администрации, подтвердивший, что Федеральное управление гражданской авиации входит в число агентств, пострадавших от взлома, сказал, что ответ агентству помешала устаревшая технология, и он неделями пытался определить, на скольких серверах установлено программное обеспечение SolarWinds.

FAA первоначально сообщило AP в середине февраля, что оно не пострадало от взлома SolarWinds, но через несколько дней выпустило второе заявление о том, что расследование продолжается.

По крайней мере, еще один член кабинета, помимо Вольфа, пострадал. По словам одного из бывших высокопоставленных чиновников администрации, хакерам удалось получить графики чиновников Министерства энергетики, в том числе тогдашнего секретаря Дэна Бруйетта. Графики не были конфиденциальными и регулируются законами об открытых записях.

Представитель министерства энергетики Кевин Ляо заявил, что «не нашло доказательств того, что сеть, которая поддерживает графики высокопоставленных чиновников, была скомпрометирована».

Новые раскрытия информации дают более полное представление о том, какие данные были получены при взломе SolarWinds. По этому поводу было проведено несколько слушаний в Конгрессе, но они особенно не содержали деталей.

Член палаты представителей Пэт Фэллон, штат Техас, указал на одном из слушаний, что электронная почта секретаря DHS была взломана, но не предоставил дополнительных подробностей. AP удалось идентифицировать Вольфа, который отказался от комментариев, кроме того, что у него было несколько учетных записей электронной почты в качестве секретаря.

Представитель DHS Сара Пек заявила, что «взлома была совершена небольшая часть учетных записей сотрудников» и что агентство «больше не видит индикаторов взлома в наших сетях».

Администрация Байдена пообещала в ближайшее время издать указ, чтобы устранить «значительные пробелы в модернизации и технологиях

кибербезопасности в федеральном правительстве». Но список препятствий, с которыми сталкивается федеральное правительство, обширен: высококвалифицированные иностранные хакеры, поддерживаемые правительствами, которые не боятся репрессий США, устаревшие технологии, нехватка обученных профессионалов в области кибербезопасности и сложная структура руководства и надзора.

Недавно одобренный пакет стимулов включает в себя 650 миллионов долларов в виде новых денег для Агентства по кибербезопасности и безопасности инфраструктуры для усиления киберзащиты страны. Федеральные чиновники заявили, что эта сумма является лишь первоначальным взносом на гораздо более крупные запланированные расходы на улучшение обнаружения угроз.

«Мы должны повысить нашу игру», - сказал Брэндон Уэльс, возглавляющий агентство по кибербезопасности, на недавних слушаниях в комитете Палаты представителей.

Агентство использует систему обнаружения угроз, известную как Эйнштейн. Неспособность обнаружить брешь в SolarWinds до того, как она была обнаружена частной охранной компанией, встревожила чиновников. Эрик Голдштейн, заместитель исполнительного директора агентства по кибербезопасности, сообщил Конгрессу, что технология Эйнштейна была разработана десять лет назад и «несколько устарела».

Энтони Ферранте, бывший директор по реагированию на киберинциденты Совета национальной безопасности США и нынешний старший управляющий директор FTI Consulting, сказал, что отчасти проблема, как в правительстве, так и в частном секторе, заключается в нехватке квалифицированной рабочей силы.

Взлом Microsoft Exchange, который на сегодняшний день не затронул никакие федеральные правительственные учреждения, также был обнаружен частной фирмой.

Одна из проблем, которая ставит в тупик политиков, заключается в том, что хакеры из иностранных государств все чаще используют виртуальные частные сети, или VPN, базирующиеся в США, чтобы избежать обнаружения американскими спецслужбами, которые по закону ограничены в мониторинге внутренней инфраструктуры. Как недавно заявили официальные лица, хакеры SolarWinds использовали услуги хостинга Amazon Web Services и GoDaddy, чтобы избежать обнаружения.

Администрация Байдена не планирует в ответ усилить государственное наблюдение за Интернетом в США, а вместо этого хочет сосредоточиться на более тесном партнерстве и улучшении обмена информацией с компаниями частного сектора, которые уже имеют широкую видимость внутреннего Интернета.

Ответственность за реагирование на нарушения, предотвращение новых и обеспечение надзора за этими усилиями все еще не решена, и в прошлом месяце лидеры сенатского комитета по разведке сначала раскритиковали администрацию Байдена за «неорганизованный ответ» на взлом SolarWinds до того, как Белый дом выступил с заявлением. уточнение структуры его руководства.

Администрация Байдена обратилась к Анне Нойбергер, заместителю советника по национальной безопасности по кибербезопасности и технологиям в

чрезвычайных ситуациях, чтобы она отреагировала на взломы SolarWinds и Microsoft. Он не назначил национального кибердиректора - новая должность, что расстраивает некоторых членов Конгресса.

«Мы пытаемся вести войну с несколькими фронтами без чьей-либо ответственности», - сказал сенатор Ангус Кинг, независимый от штата Мэн.

Администрация Байдена заявляет, что рассматривает, как лучше всего создать новую позицию. «Кибербезопасность - главный приоритет», - заявила представитель Белого дома Эмили Хорн». ***(ALAN SUDERMAN. AP sources: SolarWinds hack got emails of top DHS officials // THE ASSOCIATED PRESS (https://apnews.com/article/solarwinds-hack-email-top-dhs-officials-8bcd4a4eb3be1f8f98244766bae70395). 29.03.2021).***

***

Кіберзахист критичної інфраструктури

«В рамках более широкой стратегии повышения устойчивости инфраструктуры Австралии к кибербезопасности правительство 10 декабря 2020 года внесло в парламент законопроект о внесении поправок в законодательство о безопасности (критическая инфраструктура). В ответ на ряд запросов клиентов о последствиях законопроекта, мы даем краткое описание.

Ключевые выводы

Законопроект предлагает существенно расширить сферу применения Закона о безопасности критической инфраструктуры 2018 (Cth) (Закон SOCI) на 11 секторов критической инфраструктуры

Законопроект наделяет федеральное правительство более широкими полномочиями, включая возможность вмешиваться и направлять организации для предоставления информации или выполнения определенных действий при реагировании на инциденты кибербезопасности и предлагаемые новые обязательства включают: «позитивное обязательство по обеспечению безопасности» для критически важной инфраструктуры, включая обязательную отчетность о киберинцидентах и программу управления рисками;

и повышенные обязательства по кибербезопасности для систем, которые считаются имеющими «национальное значение».

Кто подлежит изменениям?

Закон SOCI в настоящее время применяется к операторам активов только в четырех важнейших инфраструктурных секторах - электроэнергетике, газе, воде и портах.

Законопроект вводит расширенное определение «сектора критической инфраструктуры», которое расширяет сферу применения Закона SOCI до 11 классов критической инфраструктуры, включая:

коммуникации;

хранение и обработка данных;

оборона;

финансовые услуги и рынки;

еда и бакалея;

здравоохранение и медицина;

транспорт;

высшее образование и исследования;

энергия;

космическая техника; и

вода и канализация.

Какие новые обязательства?

Положительные обязательства по обеспечению безопасности

Законопроект вводит позитивные обязательства в области безопасности, если министр внутренних дел (министр) принял правило или постановление о включении конкретного обязательства для конкретных критически важных объектов инфраструктуры. Эти позитивные обязательства по обеспечению безопасности могут потребовать от организаций:

принять, соблюдать и регулярно пересматривать программу управления рисками критически важной инфраструктуры с учетом всех опасностей;

сообщать об инцидентах кибербезопасности в Австралийское управление сигналов (в течение 12 или 24 часов, в зависимости от степени критичности); и

предоставлять информацию о праве собственности и операционную информацию в Реестр важнейших инфраструктурных активов.

Системы национального значения

Министр может объявить критически важный объект инфраструктуры «системой национального значения» с учетом характера и степени взаимозависимостей между активом и другими критически важными объектами инфраструктуры. На данном этапе никаких систем государственного значения не заявлено.

Если организация объявлена системой национального значения, на нее могут распространяться повышенные обязательства в области кибербезопасности, включая требования к:

принимать, соблюдать, регулярно пересматривать и предоставлять министру внутренних дел (секретарю) план реагирования на инциденты кибербезопасности;

провести учения по кибербезопасности, чтобы проверить готовность к реагированию и смягчить их, и предоставить секретарю отчет об оценке;

провести оценку уязвимости и сообщить об этом секретарю; и

предоставить Правительству доступ к системной информации (за исключением личной информации).

Важно отметить, что если секретарь считает, что ответственное лицо технически не способно подготовить такие отчеты о системной информации, секретарь может потребовать от организации установить и поддерживать указанную компьютерную программу для сбора, записи и передачи необходимой системной информации.

Распоряжения и запросы правительства

Законопроект вводит режим государственной помощи, который позволяет секретарю вводить одно или несколько из следующих указаний и запросов во

время и после кибератаки, которая серьезно подрывает социальную или экономическую стабильность или национальную безопасность Австралии:

руководство по сбору информации - указание организации раскрыть секретарю информацию, которая может помочь в определении того, следует ли осуществлять полномочия в соответствии с Законом о SOCI (с поправками, внесенными в законопроект) в отношении инцидента / актива;

направление действия - указание субъекту выполнить одно или несколько определенных действий или действий в ответ на инцидент; или же

запрос на вмешательство - запрос на вмешательство Австралийского управления связи для выполнения одного или нескольких предписанных действий или действий (например, доступ, изменение или анализ компьютерных систем или данных)

Каковы основные проблемы отрасли?

Противоречивые приоритеты

Организации выразили озабоченность по поводу законопроекта, в частности, по поводу новых полномочий правительства по прямому действию и широкого круга организаций, которые подпадут под действие новых правил (независимо от их связи с традиционным сектором инфраструктуры).

Бизнес и правительство имеют разные приоритеты при кибератаке, в том числе:

Частный сектор - возобновите бизнес как можно скорее; содержать последствия нарушения; избежать репутационного ущерба.

Правительство - усиление партнерства между государством и промышленностью; защищать национальные интересы.

Ограниченные права на апелляцию / пересмотр

Организации имеют ограниченные права обжаловать решение о наложении указаний и запросов - например, в обстоятельствах, когда организация считает, что указание или запрос не является ни соразмерным, ни разумно необходимым, или когда соблюдение указаний технически невозможно.

Министр и секретарь не обязаны консультироваться с затронутым лицом, если это может подорвать эффективность разрешения, распоряжения или запроса.

Судебный надзор в соответствии с Законом 1977 года об административных решениях (судебный надзор) (Cth) недоступен для таких решений (по соображениям национальной безопасности и озабоченности по поводу обнародования информации об инцидентах кибербезопасности)…» ***(Anthony Cooke, John Moran. Changes to the Security of Critical Infrastructure Act // Clyde & Co LLP (https://www.clydeco.com/en/insights/2021/03/changes-to-the-security-of-critical-infrastructure). 25.03.2021).***

***

«В недавнем исследовании излагается ряд проблем с конфиденциальностью, связанных с программами, с которыми пользователи взаимодействуют при использовании голосового помощника Amazon, Alexa. Проблемы варьируются от вводящей в заблуждение политики конфиденциальности до способности третьих лиц изменять код своих программ после получения одобрения Amazon.

«Когда люди используют Alexa для игр или поиска информации, они часто думают, что взаимодействуют только с Amazon», - говорит Анупам Дас, соавтор статьи и доцент кафедры информатики в Университете штата Северная Каролина. «Но многие приложения, с которыми они взаимодействуют, были созданы третьими сторонами, и мы выявили несколько недостатков в текущем процессе проверки, которые могут позволить этим третьим сторонам получить доступ к личной или частной информации пользователей».

Речь идет о программах, которые работают на Alexa и позволяют пользователям делать все, от прослушивания музыки до заказа продуктов. Эти программы, которые примерно эквивалентны приложениям на смартфоне, называются навыками. Amazon продала не менее 100 миллионов устройств Alexa (а возможно, в два раза больше), и пользователи могут выбирать из более чем 100 000 навыков. Поскольку большинство этих навыков создается сторонними разработчиками, а Alexa используется дома, исследователи хотели узнать больше о потенциальных проблемах безопасности и конфиденциальности.

С этой целью исследователи использовали автоматизированную программу для сбора 90 194 уникальных навыков, которые можно найти в семи различных магазинах навыков. Исследовательская группа также разработала автоматизированный процесс проверки, который предоставил подробный анализ каждого навыка.

Одна из проблем, которую отметили исследователи, заключалась в том, что в магазинах навыков отображается разработчик, ответственный за публикацию навыка. Это проблема, потому что Amazon не проверяет правильность имени. Другими словами, разработчик может претендовать на звание кого угодно. Это упростит злоумышленнику регистрацию от имени более надежной организации. Это, в свою очередь, может заставить пользователей думать, что навык опубликован заслуживающей доверия организацией, что облегчает фишинговые атаки.

Исследователи также обнаружили, что Amazon позволяет нескольким навыкам использовать одну и ту же фразу вызова.

«Это проблематично, потому что, если вы думаете, что активируете один навык, но на самом деле активируете другой, это создает риск того, что вы поделитесь информацией с разработчиком, с которым вы не собирались делиться информацией», - говорит Дас. «Например, для некоторых навыков требуется привязка к сторонней учетной записи, такой как учетная запись электронной

почты, банковского счета или социальной сети. Это может создать значительную угрозу конфиденциальности или безопасности для пользователей».

Кроме того, исследователи продемонстрировали, что разработчики могут изменять код в конце навыков после того, как навык был размещен в магазинах. В частности, исследователи опубликовали навык, а затем изменили код, чтобы запрашивать дополнительную информацию у пользователей после того, как навык был одобрен Amazon.

«Мы не участвовали в злонамеренных действиях, но наша демонстрация показывает, что недостаточно средств контроля, чтобы предотвратить злоупотребление этой уязвимостью», - говорит Дас.

У Amazon есть некоторые меры защиты конфиденциальности, в том числе явные требования, касающиеся восьми типов личных данных, включая данные о местоположении, полные имена и номера телефонов. Одно из этих требований заключается в том, что у любых навыков, запрашивающих эти данные, должна быть действующая публично доступная политика конфиденциальности, объясняющая, почему навык хочет эти данные и как навык будет использовать эти данные.

Но исследователи обнаружили, что 23,3% из 1146 навыков, которые запрашивали доступ к конфиденциальным данным, либо не имели политики конфиденциальности, либо их политики конфиденциальности вводили в заблуждение или были неполными. Например, некоторые запрашивали личную информацию, даже если в их политике конфиденциальности говорилось, что они не запрашивали личную информацию.

Исследователи также дают ряд рекомендаций о том, как сделать Alexa более безопасным и дать пользователям возможность принимать более обоснованные решения о своей конфиденциальности. Например, исследователи рекомендуют Amazon проверять личность разработчиков навыков и использовать визуальные или звуковые подсказки, чтобы пользователи знали, когда они используют навыки, которые не были разработаны самой Amazon…». ***(Study Reveals Extent of Privacy Vulnerabilities with Amazon's Alexa // Newswise (https://www.newswise.com/articles/study-reveals-extent-of-privacy-vulnerabilities-with-amazon-s-alexa). 04.03.2021).***

***

«Кибератака на SITA, почти повсеместного поставщика авиационных услуг, поставила под угрозу данные о часто летающих пассажирах многих авиакомпаний.

Компания SITA, поставщик средств связи и ИТ для 90 процентов авиакомпаний мира, подверглась взлому, поставив под угрозу данные о пассажирах, хранящиеся на серверах компании в США, в результате того, что компания называет «очень изощренной атакой».

Как сообщила Threatpost пресс-секретарь компании Эдна Эйме-Яхиль, пострадавшие серверы находятся в Атланте и относятся к системе обслуживания пассажиров SITA (SITA PSS). SITA PSS управляет системами обработки данных о

пассажирах авиакомпаний и принадлежит группе компаний SITA со штаб-квартирой в ЕС.

Malaysia Air и Singapore Airlines в последние дни уже попали в заголовки газет после того, как предупредили своих клиентов, что они были скомпрометированы в результате атаки.

…Singapore Airlines сообщила, что только клиентов затронуто более 580 000, что означает, что компрометация может в конечном итоге затронуть миллионы пользователей.

«Каждой пострадавшей авиакомпании была предоставлена подробная информация о точном типе данных, которые были скомпрометированы, включая сведения о количестве записей данных в каждой из соответствующих категорий данных», - сказала Яхиль.

Данные о часто летающих пассажирах взломаны

Хотя компания не комментировала конкретно типы раскрываемых данных, «за исключением того, что они включают некоторые личные данные пассажиров авиакомпаний», - добавил Яхиль. «Многие авиакомпании опубликовали публичные заявления, подтверждающие, какие типы данных были затронуты в отношении их пассажиров».

Авиакомпании-члены Star Alliance, включая Luthansa, New Zealand Air и Singapore Airlines, а также члены OneWorld Cathay Pacific, Finnair, Japan Airlines и Malaysia Air, уже начали общаться со своими пользователями из группы риска. South Данные о пассажирах корейской авиакомпании JeJu Air также были скомпрометированы.

«Инцидент с безопасностью данных произошел в нашем стороннем поставщике ИТ-услуг, а не в компьютерных системах Malaysia Airlines», - говорится в Twitter-аккаунте Malaysia Air о взломе, без упоминания SITA по имени. «Тем не менее, авиакомпания отслеживает любую подозрительную деятельность, касающуюся учетных записей своих участников, и находится в постоянном контакте с пострадавшим поставщиком ИТ-услуг, чтобы обезопасить данные участников и расследовать масштабы и причины инцидента».

Системы связаны через SITA PSS, поэтому одна авиакомпания может признавать преимущества для часто летающих пассажиров от других перевозчиков.

«SITA PSS хранила данные авиакомпаний, которые не являются ее прямыми клиентами, но являются членами альянса, потому что другие авиакомпании, являющиеся клиентами SITA PSS, обязаны признавать статус часто летающих пассажиров и обеспечивать, чтобы такие пассажиры получали соответствующие привилегии, когда они летят с ними», - объяснила Яхиль Threatpost. «Это обязательство вытекает из договорных обязательств, которые другая авиакомпания согласовала в своих договорных соглашениях с альянсной организацией»…

Число атак на цепочку поставок авиакомпаний растет

Хотя подробностей о том, как произошла атака, мало, архитектор решений HackerOne Шломи Либеров сказал, что «клад» в виде личных данных SITA будет дразнить киберпреступников.

«Пока не ясно, какой вектор атаки был в взломе SITA, но данные об уязвимостях HackerOne показывают, что авиационная и аэрокосмическая

промышленность видит больше уязвимостей повышения привилегий и SQL-инъекций, чем любая другая отрасль, что составляет 57% уязвимостей, о которых сообщалось, компании этичными хакерами», - пояснил Либеров. «SITA может стать привлекательной мишенью для преступников из-за конфиденциального характера информации, которой они владеют - имен, адресов, паспортных данных».

Либеров добавил, что авиакомпаниям пора заняться защитой своих систем.

Блокировка цепочки поставок программного обеспечения

Это нарушение является еще одним в длинном списке недавних жестоких атак на сторонних поставщиков цепочек поставок, направленных на более крупные и безопасные организации. Самым известным недавним событием является нарушение правительства США SolarWinds; а также существует волна глобальных атак нулевого дня на пользователей устаревшего продукта Accellion File Transfer Appliance.

«Увеличивающийся эффект атаки на SITA - еще один пример того, насколько уязвимыми могут быть организации исключительно на основании их связей со сторонними поставщиками», - сказал Ран Нахмиас, соучредитель Cyberpion. «Если такие, казалось бы, законные соединения не контролируются и не защищаются должным образом, они могут привести к серьезным нарушениям, приводящим к раскрытию очень конфиденциальных данных, как свидетельствует эта ситуация».

Это означает, что ИТ-команды должны оценить безопасность каждой компании в пределах их периметра, сказала Деми Бен-Ари из Panorays.

«Вы просто не сможете узнать, соответствуют ли ваши третьи стороны мерам безопасности вашей компании и готовы ли они к риску, пока вы не завершите полную оценку безопасности поставщика, - пояснил Бен-Ари. «Но с помощью автоматизированных анкет, оценок внешнего воздействия и принимая во внимание влияние взаимоотношений на бизнес, вы можете получить четкую и актуальную картину рисков безопасности поставщика. Важно отметить, что лучшая практика - это не одноразовое действие, а непрерывный мониторинг в реальном времени».

Дэвид Уилер, директор открытого источника безопасности цепи поставок в Linux Foundation, пояснил… как заблокировать цепочку поставок, что подкованные айтишники должны начать с просьбой о SBOMs или о подсчете программного обеспечения, перед использованием любого стороннего решения. Это поможет гарантировать, что платформа была написана безопасно и с надежным кодом…». ***(Becky Bracken. Massive Supply-Chain Cyberattack Breaches Several Airlines // Threatpost (https://threatpost.com/supply-chain-cyberattack-airlines/164549/). 05.03.2021).***

***

«Фишинговая атака, нацеленная на пользователей Microsoft, использует поддельную систему Google reCAPTCHA.

На пользователей Microsoft распространяются тысячи фишинговых писем в ходе продолжающейся атаки с целью кражи их учетных данных Office 365. Злоумышленники придают кампании вид легитимности, используя поддельную систему Google reCAPTCHA и целевые страницы доменов верхнего уровня, на которых размещены логотипы компаний жертв.

По данным исследователей, за последние три месяца не менее 2500 таких электронных писем были безуспешно отправлены высокопоставленным сотрудникам банковского и ИТ-сектора. Письма сначала перенаправляют получателей на поддельную страницу системы Google reCAPTCHA. Google reCAPTCHA - это сервис, который помогает защитить веб-сайты от спама и злоупотреблений, используя тест Тьюринга для различения людей и ботов (например, предлагая пользователю щелкнуть пожарный гидрант из серии изображений).

После того, как жертвы «проходят» тест reCAPTCHA, они перенаправляются на фишинговую целевую страницу, которая запрашивает их учетные данные Office 365.

«Атака примечательна тем, что нацелена на высших руководителей бизнеса с такими званиями, как вице-президент и управляющий директор, которые, вероятно, будут иметь более высокий уровень доступа к конфиденциальным данным компании», - заявили исследователи из группы исследования безопасности Zscaler ThreatLabZ. «Цель этих кампаний - украсть учетные данные этих жертв, чтобы позволить злоумышленникам получить доступ к ценным активам компании».

Поддельные фишинговые письма: вложения голосовой почты

Фишинговые письма представляют собой автоматические электронные письма от средств унифицированных коммуникаций жертв, в которых говорится, что у них есть вложение голосовой почты. Например, в одном электронном письме пользователям сообщается, что «(503) *** - 6719 оставил вам сообщение длительностью 35 секунд 20 января» вместе с одиночным вложением под названием «vmail-219.HTM». Другой сообщает получателям электронной почты: «ПРОСМОТРЕТЬ БЕЗОПАСНЫЙ ДОКУМЕНТ».

Когда жертвы нажимают на вложение, они затем сталкиваются с поддельным экраном Google reCAPTCHA, который содержит типичное поле reCAPTCHA с флажком, который пользователь должен щелкнуть, с надписью «Я не робот», который затем запускает тест Тьюринга.

После заполнения поддельной системы reCAPTCHA жертвы направляются к тому, что выглядит как экран входа в систему Microsoft. Страницы входа также содержат различные логотипы компаний, в которых работают жертвы - например, один содержит логотип компании-разработчика программного обеспечения ScienceLogic, а другой - компании по аренде офисов BizSpace. Это показывает, что злоумышленники выполнили свою домашнюю работу и настраивают свои фишинговые целевые страницы в соответствии с профилем своих жертв, чтобы атака выглядела более законной.

Жертв просят ввести свои учетные данные в систему; как только они это сделают, им будет сообщено, что проверка прошла успешно и что они перенаправляются.

Исследователи обнаружили множество фишинговых страниц, связанных с кампанией, которые размещались с использованием общих доменов верхнего уровня, таких как .xyz, .club и .online. Эти домены верхнего уровня обычно используются киберпреступниками для спама и фишинговых атак. Это потому, что

их можно купить менее чем за 1 доллар каждый - низкая цена для повышения уровня достоверности фишинговых кампаний.

Больше фишинговых атак на поддельную тактику Google reCAPTCHA

Злоумышленники годами использовали фиктивные системы reCAPTCHA в своих атаках. Например, в 2019 году вредоносная кампания была нацелена на польский банк и его пользователей с помощью электронных писем, содержащих ссылку на вредоносный файл PHP, который в конечном итоге загрузил вредоносное ПО BankBot в системы жертв. Для большей реалистичности злоумышленники использовали поддельную систему Google reCAPTCHA.

Другая фишинговая атака в феврале, якобы отправленная из службы голосовой почты, содержала ссылку для воспроизведения голосового сообщения «Play Audi Date.wav», в конечном итоге перенаправляя жертв на вредоносный сайт с сообщением reCAPTCHA.

Оба приведенных выше примера показывают, что reCAPTCHA продолжает использоваться в фишинговых атаках, поскольку эта тактика успешно добавляет легитимности атаке: «Подобные фишинговые кампании с использованием поддельных reCAPTCHA Google наблюдались в течение нескольких лет, но эта конкретная кампания нацелена на руководителей в конкретной отрасли, вертикали, стартовали в декабре 2020 года», - отмечают исследователи.

Пользователи Microsoft Office 365 столкнулись с несколькими изощренными фишинговыми атаками и мошенничеством за последние несколько месяцев. В октябре исследователи предупредили о фишинговой кампании, которая выдавала себя за автоматическое сообщение от Microsoft Teams. На самом деле атака была направлена на кражу учетных данных получателей Office 365. Также в октябре фишинговая атака с использованием учетных данных Office365 была нацелена на гостиничный бизнес с использованием визуальных CAPTCHA, чтобы избежать обнаружения и выглядеть легитимными. Фишинговые злоумышленники также применили новую тактику, такую как Google Translate или пользовательские шрифты, чтобы мошенничество выглядело более законным». ***(Lindsey O'Donnell. Fake Google reCAPTCHA Phishing Attack Swipes Office 365 Passwords // Threatpost (https://threatpost.com/google-recaptcha-phishing-office-365/164566/). 08.03.2021).***

***

«Налогоплательщики США становятся жертвами фишинговых атак, пытающихся захватить их компьютеры с помощью вредоносных программ и украсть конфиденциальную личную и финансовую информацию.

По данным Казначейства, IRS получило более 141 миллиона деклараций по индивидуальному подоходному налогу [PDF] в течение сезона подачи документов 2019 года, при этом примерно 90,4 процента из них (около 127 миллионов) были поданы в электронном виде.

«Социальная инженерия с помощью фишинговых писем по-прежнему является предпочтительным методом заражения как среди киберпреступников, так и среди субъектов угроз со стороны государства», - сказал Ассаф Дахан, старший директор и руководитель отдела исследования угроз Cybereason.

«Возможен серьезный ущерб, и вредоносное ПО позволяет злоумышленникам получить полный контроль над машиной жертвы и украсть конфиденциальную информацию у пользователей или их работодателей».

У этой продолжающейся фишинг-кампании будет больше времени для заражения налогоплательщиков вредоносным ПО, поскольку в среду Министерство финансов и налоговая служба (IRS) объявили, что срок подачи налоговой декларации по федеральному подоходному налогу для физических лиц будет продлен еще на 30 дней до 17 мая 2021 года.

Обнаружение уклонения с помощью стеганографии, загрузки неопубликованных библиотек DLL и законного злоупотребления платформой

Злоумышленники отправляют электронные письма с вложениями вредоносных документов, замаскированных под налоговые документы, с просьбой к потенциальным жертвам разрешить редактирование, как подробно описано в отчете, опубликованном сегодня командой Cybereason Nocturnus.

Вместо этого это позволит встроенным макросам загружать загрузчик вредоносных программ, который использует боковую загрузку DLL для развертывания и запуска полезной нагрузки NetWire или Remcos, скрытой внутри файла изображения, размещенного в облачной службе хранения изображений imgur.

Вредоносные документы также уклоняются от традиционных антивирусных вирусов и эвристического обнаружения, злоупотребляя службой imgur для размещения полезных нагрузок вредоносных программ, что еще больше затрудняет обнаружение и блокирование их атак.

«Использование различных методов, таких как стеганография, хранение полезной нагрузки в законных облачных сервисах и использование неопубликованной библиотеки DLL против легитимного программного обеспечения, делает эти кампании очень трудными для обнаружения», - добавил Дахан.

«Конфиденциальная информация, полученная от жертв, может быть продана подпольным сообществам и использована для осуществления всех видов кражи личных данных и финансового мошенничества».

Вредоносное ПО RAT использовалось для захвата устройств налогоплательщиков

NetWire и Remcos - это два хорошо известных коммерческих трояна удаленного доступа (RAT), распространяемых по модели Malware-as-a-Service (MaaS) на основе подписки.

Оба штамма RAT были замечены в атаках, координируемых спонсируемыми государством хакерскими группами и финансово мотивированными участниками угроз.

Они предоставляют злоумышленникам функции кейлоггинга и кражи паролей, а также возможности удаленного управления, которые позволяют им взять под контроль взломанные устройства.

Были замечены мошенники, выдающие себя за IRS в электронных письмах, пытающихся обманом заставить жертв выплатить сфабрикованные невыплаченные

суммы, связанные с пропущенными или просроченными платежами, и угрожать им судебными обвинениями.

Конфиденциальная информация, собранная в ходе таких фишинговых кампаний, впоследствии может быть использована для кражи личных данных и налогового мошенничества.

Федеральная торговая комиссия США (FTC) в прошлом месяце предупредила, что количество сообщений о краже личных данных удвоилось в течение 2020 года по сравнению с 2019 годом, достигнув рекордного уровня в 1,4 миллиона сообщений в течение одного года». ***(Sergiu Gatlan. US taxpayers targeted with RAT malware in ongoing phishing attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/us-taxpayers-targeted-with-rat-malware-in-ongoing-phishing-attacks/). 18.03.2021).***

***

«В 2020 году количество штрафов и компенсационных выплат за нарушения, приведшие к утечкам данных и другой конфиденциальной пользовательской информации, по сравнению с 2019 годом выросло на 9,3%. Их общая сумма в 2020 году составила около $385 млн.

Экспертно-аналитический центр ГК InfoWatch провел исследование финансовых последствий инцидентов, связанных с утечками персональных данных и другой конфиденциальной пользовательской информации, для юридических лиц. На основе изучения открытых источников в мире было обнаружено 118 случаев назначения штрафов и компенсационных выплат за нарушения, приведшие к утечкам данных.

В 2020 году лидерами по числу штрафов стали США и Сингапур - на них пришлись, соответственно, 28 и 23 финансовых взыскания. В первую пятерку стран по количеству назначенных взысканий также вошли Румыния (11 штрафов), Италия (9 штрафов) и Соединенное Королевство Великобритании и Северной Ирландии (5 штрафов). Как и годом ранее, США заняли первое место среди стран по размеру среднего штрафа. Его сумма в 2020 году составила $13 млн.

Число штрафов, вынесенных регуляторами стран Евросоюза за утечки, составило 35,6% от всех штрафов, но средний штраф здесь составил только $93 тыс.

В России за исследуемый период в открытых источниках обнаружены сообщения о 4 штрафах за утечки персональных данных на общую сумму 510,5 тысяч рублей. Таким образом, по сравнению с 2019 годом, когда было выявлено 6 назначенных штрафов на общую сумму 180,5 тысяч рублей, в 2020 году сумма штрафов выросла в 2,83 раза. Средняя сумма штрафа составила 127,6 тыс. рублей.

В 2020 году российские суды вынесли решения о назначении штрафов по делам, возбужденным в отношении таких организаций, как одно из коллекторских агентств в Новосибирской области, ООО «Национальная служба взыскания», Центр немецкого языка при Волгоградском социально-педагогическом университете, а также Центральная районная больница города Николаевск-на-Амуре.

«Данное исследование проводилось в двух срезах, где первая часть – это подсчет фактического количества штрафов и компенсаций, назначенных регуляторами за утечки конфиденциальной информации, в том числе персональных данных. Вторая часть - поиск связи между финансовым состоянием организации, стоимостью её активов и официальными сообщениями об утечках. Совершенно очевидно, что для публичной компании как сам факт утечки, так и информация о ее масштабе, ставшие достоянием общественности, чреваты потерями на бирже. По нашим наблюдениям, после утечки компании в среднем в первые часы после объявления об инциденте падение выглядит небольшим, в пределах 1%, но нельзя забывать, что за этой цифрой для крупной компании стоит потеря многих десятков, а то и сотен миллионов долларов. Немаловажным фактором, влияющим на возможность нивелирования репутационных рисков и стабилизацию стоимости акций, является поведение самой компании после утечки, прозрачность мероприятий для ликвидации последствий инцидента», - отмечает руководитель направления аналитики и спецпроектов ГК InfoWatch Андрей Арсентьев.

В отраслевом распределении 50% мировых штрафов пришлись на хайтек-компании, здравоохранение и ритейл. Наибольшее падение биржевых показателей сразу после утечек отмечено среди компаний сегментов «Ритейл&HoReCa», а также «Высокие технологии» (хайтек - телеком, ИТ) – на 2,29% и 2,02% соответственно. Наименее восприимчива к утечкам сфера промышленности и транспорта – здесь даже после инцидента, связанного с компрометацией данных, курс акций в среднем подрастал на 0,56%. Относительно устойчивой также можно признать финансовую сферу, потери участников которой в первые часы после утечки оказались довольно невелики – менее четверти процента.

На сегодня можно достаточно уверенно говорить о том, что утечка оказывает сильное влияние на уровень капитализации компании в краткосрочной перспективе, то есть в первые дни после сообщения об инциденте. В дальнейшем на формирование курса акций влияют другие факторы.

Авторы отчета пришли к выводу, что регуляторы стран ЕС, опираясь на положения вступившего в силу в 2018 году регламента GDPR, в 2020 году продолжили методично штрафовать компании, допустившие утечки. При этом в Евросоюзе в период пандемии практически нет крупных штрафов за утечки. Скорее всего, в ближайшее время мега-штрафы (в размере десятков и сотен миллионов долларов) в основном будут выписываться регуляторами США и только за резонансные утечки, то есть те, при которых могут быть потеряны миллионы записей пользовательских данных. При этом отягчающими факторами будут выступать длительное сокрытие фактов утечек и недостаточное внимание компаний к контуру кибербезопасности.

В 2021 году, прежде всего, стоит ожидать расширения географии штрафов за утечки по причине того, что регуляторы в сфере защиты информации во многих странах постепенно совершенствуют законодательство, исходя из новых реалий, и встают на путь методичной защиты пользовательских данных как основного компонента цифровой личности.

В России следует ожидать появления штрафов, связанных с обеспечением безопасности значимых объектов критической информационной инфраструктуры

(не утечки)». ***(В мире стали чаще штрафовать за утечки персональных данных // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5723654-V-mire-stali-chashhe-shtrafovat.html). 11.03.2021).***

***

«11 марта губернатор штата Юта подписал контракт HB 80., который обеспечивает организациям надежную защиту от утечки данных, если они соблюдают определенные отраслевые стандарты кибербезопасности. Среди прочего, «лицо, которое создает, поддерживает и в разумных пределах соблюдает письменную программу кибербезопасности», которая отвечает конкретным требованиям безопасности для защиты личной информации и находится на месте во время утечки данных, имеет положительную защиту от претензий, поданных в соответствии с Ютой. закона или в судах штата, которые утверждают, что лицо не реализовало разумные меры защиты информации, что привело к утечке данных. Лицо также имеет положительную защиту от претензий относительно неспособности надлежащим образом отреагировать на нарушение данных или предоставить уведомление затронутым лицам, если письменная программа кибербезопасности содержала конкретные протоколы на момент нарушения, которые «в разумной степени соответствовали требованиям для письменная программа кибербезопасности» для реагирования на утечку данных или для направления уведомления. HB 80 также описывает компоненты, которые письменная программа кибербезопасности должна включать в себя, чтобы иметь право на утвердительную защиту, и вступает в силу через 60 дней после закрытия заседания законодательного органа». ***(Utah creates certain affirmative defenses for data breaches // Buckley LLP (https://buckleyfirm.com/blog/2021-03-25/utah-creates-certain-affirmative-defenses-data-breaches#page=1). 25.03.2021).***

***

«Инженер по безопасности и бывший участник некоммерческой организации по открытым системам недавно сообщил об утечке данных в организацию.

В свою очередь, его сначала поблагодарили за ответственный репортаж, но позже он получил известие от их адвокатов и полиции.

Apperta Foundation - британская некоммерческая организация, поддерживаемая NHS England и NHS Digital, которая продвигает открытые системы и стандарты в области цифрового здравоохранения и социальной помощи.

Репозиторий GitHub предоставляет пароли, ключи, базу данных

На этой неделе британский инженер по облачной безопасности Роб Дайк рассказал о том, как в случае сообщения об утечке данных с соблюдением этических норм у него возникли проблемы с законом.

Ранее в этом месяце Дайк обнаружил открытый репозиторий GitHub с паролями, ключами API и конфиденциальными финансовыми записями, принадлежащими Apperta Foundation.

Обнаружив этот репозиторий GitHub, который, по словам инженера, был общедоступным, по крайней мере, с 2019 года, инженер лично сообщил об этом Apperta и получил от них благодарность.

Однако 9 марта он получил юридическую корреспонденцию от юристов Апперты, что побудило его нанять собственных поверенных, чтобы представлять его интересы.

Кроме того, вчера было получено электронное письмо от кибер-следователя полиции Нортумбрии по поводу сообщения о «злоупотреблении компьютером».

В телефонном интервью BleepingComputer Дайк сказал нам, что, работая с Apperta в прошлом [1, 2, 3], и как человек, который в настоящее время работает в ИТ-секторе, он хорошо знаком как с установленным механизмом Apperta, так и с отраслевыми практиками, когда это касается. ответственно сообщать поставщикам об уязвимостях системы безопасности.

Когда он обнаружил утечку данных, Дайк немедленно сообщил об этом Апперте.

Однако, чтобы записать то, что он сообщил, исследователь зашифровал данные, с которыми он столкнулся, и надежно хранил их в течение 90 дней в рамках скоординированного процесса раскрытия информации.

«Я знал, как я должен был сообщить им об этом. Поэтому я сообщил им об этом в соответствии с их установленной процедурой», - сказал инженер BleepingComputer, добавив, что он получил ответ от Апперты, в котором представитель благодарит его и заявляет, что «Я разберусь с проблемой.

«И я больше не думал об этом», - продолжил Дайк.

Чуть больше недели спустя от адвокатов Апперты пришло письмо, в котором говорилось, что они считают действия Дайка «незаконными», и требовали письменного обязательства об удалении любых данных, с которыми столкнулся инженер.

Это удивило инженера, особенно с учетом того, что члены команды Apperta знали его по его прошлым вкладам.

В электронных письмах, которые видел BleepingComputer, Дайк пояснил юристам Апперты, что информация, с которой он столкнулся, просочилась на GitHub публично в течение более двух лет, а не конфиденциальные данные, полученные в результате незаконной хакерской деятельности.

Детали, собранные инженером в рамках ответственного раскрытия информации, были получены из общедоступных URL-адресов, опубликованных Apperta в Интернете.

Далее Дайк издал письменное подтверждение того, что он уничтожит любую копию репозитория, полученную из общедоступной веб-службы (GitHub), и предоставит сертификат об уничтожении.

Вчера из полицейского участка Нортумбрии пришло еще одно письмо с запросом более подробной информации о том, что полиция ссылается на сообщение о «злоупотреблении компьютером (закон)».

Инженер сказал BleepingComputer, что, по его мнению, полицейское расследование связано с инцидентом в Апперте, учитывая, что полиция Нортумбрии контролирует юрисдикцию, в которой расположены офисы Апперты.

«Я не думаю, что это способ сделать это для организации, которая продвигает открытость и все, что с этим связано: прозрачность, подотчетность и ответственность».

«Поскольку я обнаружил эту утечку и помог им, это просто не способ решить эту проблему. Я дал [им] заверение, что данные будут удалены, и они были удалены», - объяснил Дайк BleepingComputer..

Закон Великобритании о неправомерном использовании компьютеров отпугивает 80% профессионалов в области информационной безопасности

Это не первый случай, когда инженер по информационной безопасности якобы входит в серую зону Закона Великобритании о неправомерном использовании компьютеров (CMA).

Регистр неоднократно [1, 2, 3] отслеживал события в отношении Закона о неправомерном использовании компьютеров и почему снова и снова британские информационные системы. фирмы и ученые призывали к реформированию некоторых аспектов устаревшего закона.

Исследование, проведенное кампанией CyberUp, показало, что 80% специалистов по безопасности боялись нарушить закон о неправомерном использовании компьютеров в ходе своей повседневной профессиональной деятельности.

Положения Закона Великобритании о неправомерном использовании компьютеров от 1990 года обширны и обширны и могут даже рассматривать простую утечку данных как «преступление».

Даже рабочая деятельность базирующихся в Великобритании поставщиков разведывательной информации об угрозах, исследующих иностранные системы, может считаться незаконной в соответствии с законом…». ***(Ax Sharma. Engineer reports data leak to nonprofit, hears from the police // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/engineer-reports-data-leak-to-nonprofit-hears-from-the-police/). 25.03.2021).***

***

«Форум Carding Mafia, связанный с куплей-продажей похищенной финансовой информации и данных кредитных карт, был взломан хакерами. По данным сервиса для проверки скомпрометированных данных Have I Been Pwned, в результате атаки были скомпрометированы почти 300 тыс. учетных записей участников форума.

Скомпрометированная информация включала адреса электронной почты, IP-адреса, логины и хеши паролей 297 744 пользователей. На момент написания новости на форуме Carding Mafia и его общедоступном канале Telegram не было никаких предупреждений об утечке данных.

Основатель Have I Been Pwned Трой Хант (Troy Hunt) подтвердил изданию Motherboard, что взломанная база данных является легитимной. Хант также обнаружил в базе данных адреса электронной почты пользователей сервиса Mailinator. Хант проверил скомпрометированные электронные адреса с помощью функции «Забыл пароль», и выяснил, что данные распознаются как действительные. Обычно адреса электронной почты Mailinator создаются для одной

цели и не используются повторно. Тот факт, что адреса содержатся в дампе данных и также подтверждаются форумом, предполагает легитимность информации.

Специалисты издания также обнаружили на другом хакерском форуме предлагаемые бесплатно данные, предположительно украденные у Carding Mafia в январе нынешнего года…». ***(Хакеры взломали кардинг-форум Carding Mafia // SecurityLab.ru (https://www.securitylab.ru/news/517806.php). 26.03.2021).***

***

Кібербезпека Інтернету речей

«Ожидается, что принятый 4 декабря 2020 года Закон о повышении кибербезопасности Интернета вещей 2020 года («Закон об IoT») значительно улучшит кибербезопасность повсеместных устройств IoT. Поскольку к 2025 году количество устройств Интернета вещей превысит 21,5 миллиарда, Закон об Интернете вещей устанавливает стандарты и руководящие принципы кибербезопасности для приобретения и использования федеральным правительством устройств Интернета вещей, способных подключаться к Интернету. Этот Закон, а также соответствующие стандарты и руководства, разрабатываемые Национальным институтом стандартов и технологий (NIST) будет напрямую влиять на государственных подрядчиков, которые производят устройства IoT для использования федеральным правительством или которые предоставляют федеральному правительству услуги, программное обеспечение или информационные системы, использующие устройства IoT.

Это также окажет значительное косвенное влияние на организации частного сектора, покупающие устройства или системы Интернета вещей, использующие такие устройства для корпоративного использования. Действительно, Конгресс специально рассчитывал на широкий спектр побочных эффектов для частного сектора, ожидая, что пресловутый прилив поднимет все лодки. В конечном итоге организациям необходимо будет определить, будут ли они покупать и использовать устройства, программное обеспечение и системы Интернета вещей, соответствующие стандартам для федерального использования, или приобретать небезопасные или менее безопасные устройства и системы Интернета вещей. Корпорации, которые потребляют и используют устройства и системы IoT, в том числе в производстве, логистике, здравоохранении, гостиничном бизнесе и розничной торговле, должны учитывать влияние Закона об IoT на кибербезопасность организации.

Среди прочего, IoT Act содержит следующие требования:

СТАНДАРТЫ И РУКОВОДСТВА NIST ПО ИСПОЛЬЗОВАНИЮ И УПРАВЛЕНИЮ УСТРОЙСТВАМИ IoT: NIST должен публиковать стандарты и рекомендации по использованию устройств IoT федеральным правительством, включая минимальные требования к информационной безопасности для управления рисками кибербезопасности. Руководство должно касаться безопасной разработки, управления идентификацией, исправлений и управления

конфигурацией. NIST должен «учитывать соответствующие стандарты, руководящие принципы и передовые методы, разработанные частным сектором, агентствами и государственно-частными партнерствами». Как отмечалось в истории законодательства, в настоящее время не существует национального стандарта для обеспечения безопасности устройств IoT, а невозможность эффективного исправления этих устройств или установки безопасных паролей устройств, помимо других уязвимостей, представляет собой серьезную угрозу для национальной инфраструктуры и безопасности.

РУКОВОДСТВО NIST ПО РАСКРЫТИЮ И РЕШЕНИЮ УЯЗВИМОСТЕЙ УСТРОЙСТВ IoT: NIST также должен публиковать рекомендации: (a) по отчетности и публикации уязвимостей безопасности информационных систем, принадлежащих или контролируемых федеральным агентством (включая устройства IoT, принадлежащие или контролируемые агентством), и устранение таких уязвимостей; и (b) для подрядчика или субподрядчика, предоставляющего такие системы, получение информации об уязвимостях и распространение информации об устранении такой уязвимости в системе безопасности. Важно отметить, что руководящие принципы должны включать пример содержания раскрытия уязвимостей, о котором подрядчик или любой его субподрядчикдолжен «сообщать, согласовывать, публиковать илиполучать».

ВЫДАЧА ПОЛИТИК И ПРИНЦИПОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ФЕДЕРАЛЬНОГО АГЕНТСТВА: Директор Управления управления и бюджета должен проверять политику и принципы информационной безопасности агентства, основанные на стандартах и рекомендациях NIST, и при необходимости издавать политики и принципы для согласования политик и принципов с NIST. стандарты и руководства.

ИЗМЕНЕНИЯ К ФЕДЕРАЛЬНЫМ ПОЛОЖЕНИЯМ О ПРИОБРЕТЕНИЯХ: Федеральное постановление о закупках должно быть пересмотрено по мере необходимости для реализации стандартов и руководств NIST.

СООТВЕТСТВИЕ ПОДРЯДЧИКУ СТАНДАРТОВ И РУКОВОДСТВ NIST: Федеральным агентствам запрещается закупать, получать, продлевать контракт на закупку или получение или использовать устройство IoT, если главный информационный директор (CIO) агентства определяет, что использование такого устройства препятствует соответствие стандартам и рекомендациям NIST, при условии отказа от прав для определенных устройств. Этот запрет вступает в силу в декабре 2022 года, фактически предусматривая двухлетний период увеличения объемов планирования в соответствии с новыми стандартами.

NIST опубликовал проект руководства по кибербезопасности устройств IoT, период обсуждения которого закончился 26 февраля 2021 г. Согласно NIST, руководство предлагает отправную точку для производителей, которые создают устройства IoT для рынка федерального правительства, а также руководство федеральным агентствам о том, что им следует запрашивать при приобретении этих устройств…

Чтобы запланировать вступление в силу Закона об Интернете вещей в декабре 2022 года, организациям следует сделать следующее:

Производители, которые производят устройства IoT для использования федеральным правительством, должны изучить проект руководства и дождаться окончательного руководства и стандартов NIST, а также разработать соответствующие требования и документацию на уровне устройств. Им также необходимо будет спланировать разработку процессов для публичного сообщения и уменьшения уязвимостей в своих устройствах.

Федеральные подрядчики, включая поставщиков программного обеспечения и услуг, должны идентифицировать информационные системы, использующие устройства IoT, и планировать выполнение рекомендаций и стандартов NIST IoT, в том числе в своих спецификациях устройств IoT, выборе поставщиков и договорных требованиях. Решения о приобретении, закупках и заключении контрактов, принятые в ближайшие месяцы, могут повлиять на способность организации использовать безопасные устройства IoT с декабря 2022 года.

Организации, не являющиеся федеральными подрядчиками, должны учитывать, как стандарты и рекомендации NIST IoT могут повлиять на соблюдение ими законов о кибербезопасности, требующих разумных мер безопасности для защищенной информации в зависимости от вариантов использования (например, Gramm-Leach Bliley, Закон о переносимости и подотчетности медицинского страхования (HIPAA); HR7898 в качестве защиты или смягчения последствий применения HIPAA, Закона NY SHIELD, Гражданского кодекса Калифорнии §1781.5, Положения о защите данных Массачусетса, Закона Иллинойса о защите личной информации и Закона о защите биометрической информации (BIPA)), включая потенциальное влияние на оценки рисков, структуры управления рисками (включая структуры NIST - например, SP 800-53, NIST Cybersecurity Frameworki другие стандарты информационной безопасности, такие как ISO, OWASP), выбор поставщиков, закупки и заключение контрактов, процессы запроса предложений, риски цепочки поставок и обучение персонала. Организация должна идентифицировать устройства IoT, включенные в ее информационные системы, и их использование в свете руководства NIST. Директорам по информационной безопасности (CISO) и техническим директорам (CTO) следует определить, способствует ли добровольное следование запрету, действующему на их коллег из федеральных агентств, на использование несовместимых устройств и систем IoT, соблюдению и снижению рисков в организации, а также последствия невыполнения этого требования…». ***(Brian G. Cesaratto, Alexander J. Franchilli. New Internet of Things (IoT) Cybersecurity Law's Far Reaching Impacts // Epstein Becker & Green, P.C. (https://www.workforcebulletin.com/2021/03/12/new-internet-of-things-iot-cybersecurity-laws-far-reaching-impacts/). 12.03.2021).***

***

«Сенатор Эд Марки (D-MA) и член палаты представителей Тед Лью (D-CA-33) вновь представили Закон о киберщите 24 марта 2021 года. Предлагаемый закон не нов для Конгресса; Сенатор Марки и член палаты представителей Лие ранее представили Закон о киберщите как в 2017, так и в 2019 году. Однако законопроект так и не прошел на голосование ни в Палате представителей, ни в Сенате.

Как написано, Закон о киберщите призывает к созданию программы добровольной сертификации кибербезопасности для устройств Интернета вещей (IoT). Устройства IoT охватывают широкий спектр продуктов, включая сотовые телефоны, ноутбуки, камеры, умные домашние помощники, умные замки, радионяни и умные кухонные приборы, и положения Закона будут применяться к любому подключенному к Интернету потребительскому продукту, который передает данные или элементы управления. действия физического объекта или системы. Предлагаемый закон предусматривает создание консультативного комитета по кибербезопасности, состоящего из экспертов в различных областях, включая академические круги, правительство, промышленность, группы потребителей и общественность. Консультативному комитету будет поручено создать определенные критерии кибербезопасности. Если продукты IoT соответствуют этим критериям, производители могут сертифицировать их с помощью знака «Cyber Shield», позволяющего потребителям выбирать сертифицированные продукты.

Предлагаемый закон идентичен законопроекту 2019 года, который внес лишь незначительные существенные изменения в его аналог 2017 года. Эти изменения включают введение положения, позволяющего министру торговли отменить сертификацию Cyber Shield, если продукт или производитель не соответствуют критериям консультативного комитета. Кроме того, версии 2019 и 2021 требуют, чтобы генеральный инспектор Министерства торговли периодически оценивал уровень участия бизнеса в программе Cyber Shield и осведомленность общественности о этикетке Cyber Shield.

Повторное введение Закона о киберщите свидетельствует о продолжающихся усилиях законодателей по достижению прогресса в обеспечении безопасности устройств Интернета вещей. Например:

4 декабря 2020 года президент Трамп подписал Закон о совершенствовании кибербезопасности Интернета вещей от 2020 года, согласно которому устройства Интернета вещей, приобретаемые федеральным правительством, должны соответствовать минимальным стандартам безопасности.

В феврале 2021 года сопредседатели Форума Интернета вещей, представители Сьюзан ДельБене (D-WA-01) и Джон Катко (R-NY-24), повторно представили законопроект, который позволит FCC собирать данные о рост устройств Интернета вещей, зависящих от сетей 5G.

Точно так же в мае 2020 года представители Джон Джойс (R-PA-13) и Ричард Хадсон (R-NC-8) представили Закон о продвижении производства IoT, который потребует от Министерства торговли изучить и впоследствии дать рекомендации Конгрессу в отношении как внедрить устройства Интернета вещей в обрабатывающую промышленность.

В пресс-релизе, объявляющем о повторном введении Закона о киберщите, сенатор Марки заявил, что «с учетом того, что к 2025 году в наших карманах и домах будет находиться 75 миллиардов устройств Интернета вещей, кибербезопасность по-прежнему представляет прямую угрозу для экономики. процветание, конфиденциальность и глобальная безопасность». Член палаты представителей Лие добавил, что закон будет способствовать тому, чтобы

кибербезопасность стала «приоритетом как для промышленности, так и для потребителей». ***(Micaela McMurrough, Jayne Ponder. "Cyber Shield Act" Calling for IoT Device Certification Reintroduced in Congress // COVINGTON & BURLING LLP (https://www.insideprivacy.com/cybersecurity-2/cyber-shield-act-calling-for-iot-device-certification-reintroduced-in-congress/#page=1). 26.03.2021).***

***

«Недавно объявив о запуске нового Совета по кибербезопасности Великобритании, правительство Великобритании объявило о своих планах опубликовать новую Национальную стратегию искусственного интеллекта (Стратегию искусственного интеллекта) в конце этого года.

Цель стратегии ИИ - укрепить позицию Соединенного Королевства как глобального центра разработки, коммерциализации и внедрения ответственного ИИ.

Стратегия AI будет сосредоточена на следующем:

Рост экономики за счет широкого использования технологий искусственного интеллекта

Этическая, безопасная и заслуживающая доверия разработка ответственного ИИ

Устойчивость к изменениям за счет акцента на навыках, талантах, исследованиях и разработках

Секретарь по цифровым технологиям Оливер Дауден объявил о стратегии, прокомментировав: «Раскрытие возможностей ИИ - главный приоритет в нашем плане стать самым технологичным правительством за всю историю. Великобритания уже является мировым лидером в этой революционной технологии, и новая стратегия искусственного интеллекта поможет нам полностью раскрыть ее потенциал - от создания новых рабочих мест и повышения производительности до борьбы с изменением климата и предоставления более качественных государственных услуг».

Стратегия ИИ должна соответствовать общим планам правительства Великобритании по поддержке рабочих мест и экономического роста за счет увеличения инвестиций в инфраструктуру, навыки и инновации. Бизнес-секретарь Кваси Квартенг отметил: «Великобритания уже использует огромный потенциал искусственного интеллекта для улучшения всей нашей жизни - от более быстрой и эффективной диагностики заболеваний до управления отоплением в наших домах. Благодаря этой стратегии мы будем воспитывать наших пионеров в области искусственного интеллекта, чтобы ускорить вывод новых технологий на рынок, открывать высококвалифицированные рабочие места, повышать производительность и укреплять статус Великобритании как глобальной научной сверхдержавы».

Правительство Великобритании подтвердило планы рассмотреть рекомендации заинтересованных сторон в промышленности, научных кругах и гражданском обществе, включая Совет ИИ, который является независимым комитетом экспертов, консультирующим по вопросам искусственного интеллекта. В январе этого года Совет по ИИ опубликовал Дорожную карту ИИ, в которой

изложен ряд рекомендаций правительству по использованию возможностей ИИ, включая рекомендацию о создании общенациональной стратегии ИИ.

Департамент цифровых технологий, культуры, СМИ и спорта создал онлайн-платформу для частных лиц и организаций, чтобы заявить о своей заинтересованности в участии в обсуждении стратегии искусственного интеллекта». ***(MIKE PIERIDES, CHARLOTTE ROXON, KELLI A. BOYLE. National Artificial Intelligence Strategy Announced in United Kingdom // Morgan, Lewis & Bockius LLP (https://www.morganlewis.com/blogs/sourcingatmorganlewis/2021/03/national-artificial-intelligence-strategy-announced-in-united-kingdom#page=1). 29.03.2021).***

***

Кіберзлочинність та кібертероризм

«Согласно новому отчету S&P Global Ratings о рынке киберстрахования, количество кибератак растет, как и финансовые убытки, которые могут последовать за ними.

Из-за пандемии COVID-19, способствующей большей цифровизации и удаленной работе, кибер-уязвимости значительно усилились. В то время как рынок киберстрахования, безусловно, растет, S&P Global Ratings подчеркнуло, что страховщикам не хватает продуктов, необходимых для надлежащего удовлетворения ожидаемого спроса.

За 2019 - 2020 года средняя стоимость убытков от кибератак во всем мире увеличилась почти в 6 раз. Однако только 26% фирм имеют отдельный полис киберстрахования, поскольку большинство компаний полагаются на общие страховые полисы или не имеют киберстрахования вообще, согласно данным отчета Hiscox о киберготовности 2020.

В последнем отчете S&P Global Ratings о киберстраховании говорится, что киберстрахование обычно включено в существующие страховые полисы имущества или ответственности. В некоторых случаях полисы прямо не включают или не исключают киберзащиту, что приводит к «тихим кибер-убыткам» - когда страховщики несут убытки от связанных с киберпреступленями требований в страховых полисах, которые не были предназначены для покрытия киберрисков.

«Даже когда кибер-защита предусмотрена страховым полисом, отсутствие прозрачности в определении кибер-события в полисе и в его условиях создает неопределенность касательно объема такой защиты», - сказано в отчете.

S&P Global предполагает, что разработка автономных продуктов киберстрахования, в частности, автономного кибер-направления бизнеса, управляемого через киберцентр передового опыта, предложит более эффективный и оптимизированный контроль риска накопления.

Другими преимуществами являются улучшение стратегической покупки перестраховочного покрытия и создание резервов в случае возможных потерь; более оптимизированный, централизованный и скоординированный сбор данных; содействие мерам предотвращения, эффективным методам обработки жалоб и

профессиональному восстановлению данных в случае жалоб; объединение внутреннего ИТ-опыта и отдела кибербезопасности.

«Такие изменения будут иметь много преимуществ для страховщиков, главное из которых - предотвращение скопления кибер-претензий в разных сферах бизнеса, а также трудностей с обработкой таких претензий», - говорится в отчете. «Это также позволило бы страховщикам снизить риск тихого кибернетического вмешательства, а также применить централизованный и скоординированный подход к сбору данных и исследованиям, что жизненно необходимо для точного расчета страховых выплат, соответствующих риску». ***(Roxanne Libatique. Cyberattacks are soaring - How can the insurance industry keep up? // Insurance Business (https://www.insurancebusinessmag.com/uk/news/cyber/cyberattacks-are-soaring--how-can-the-insurance-industry-keep-up-248234.aspx). 03.03.2021).***

***

«Сотни британских компаний были скомпрометированы в рамках глобальной кампании, связанной с китайскими хакерами.

Фирма по кибербезопасности Eset заявила, что более 500 почтовых серверов в Великобритании могли быть взломаны, и многие компании не знают, что они стали жертвами атаки.

В связи с этим правительства по всему миру предупреждают организации о необходимости защиты своих систем.

Но некоторые эксперты опасаются, что может быть слишком поздно, поскольку как минимум 10 хакерских команд извлекают выгоду из хаоса.

Национальный центр кибербезопасности Великобритании присоединился к властям США для предупреждения о взломе, но говорит, что все еще оценивает ситуацию для британских предприятий.

Тем временем норвежские кибернетические власти активно ищут в стране компании, подверженные риску, и напрямую предупреждают их.

"Нулевой день"

Хакерская кампания была впервые объявлена Microsoft 2 марта и возложена на хакерскую группу Hafnium, поддерживаемую правительством Китая.

Microsoft заявила, что группа использовала четыре невиданных ранее хакерских метода для проникновения в почтовые системы американских компаний.

Злоумышленники нацелились на популярную почтовую систему Microsoft Exchange Server, используемую крупными корпорациями и государственными органами по всему миру.

Microsoft выпустила обновления программного обеспечения для так называемых эксплойтов «нулевого дня» и призвала клиентов установить их, чтобы защитить себя.

Однако хакерство переросло от прямого шпионажа до кризисного уровня, и в некоторых отчетах говорится, что могут пострадать десятки тысяч организаций.

"Гонка сейчас"

По данным исследователей кибербезопасности из Eset, целых 10 различных хакерских групп сейчас активно используют эксплойты нулевого дня для нацеливания на компании в 115 разных странах.

Кибер-исследователи из FireEye также подтвердили, что они обнаружили несколько групп, которые, вероятно, базировались в Китае, и использовали эксплойт на разных этапах.

«Как всегда, это сложно, но вполне вероятно, что Hafnium подарил эти «нулевые дни» санкционированным правительством группировкам, чтобы они активно использовали недостатки после того, как были обнаружены», - сказал Джейк Мур из Eset.

«Сейчас идет гонка, чтобы все пострадавшие немедленно исправили, а затем тщательно проверили любые недавние компромиссы и удостоверились, что на серверах не установлены веб-оболочки».

Падение веб-оболочки

Веб-оболочка - это фрагмент компьютерного кода, который может действовать как бэкдор в компьютерной сети.

После установки хакеры закрепляются в сети и могут либо украсть, либо шпионить за сообщениями электронной почты, либо использовать доступ для запуска более серьезных кибератак.

В глобальном масштабе Eset заявляет, что обнаружила бэкдоры на 5000 отдельных серверах, и более 500 из них находятся в Великобритании.

Специалисты по кибербезопасности спешат выяснить, какие компании были взломаны, и удалить веб-оболочки, чтобы выгнать хакеров из своих систем.

Остерегайтесь второй волны

CyberGuard Technologies заявляет, что имеет дело с 42 отдельными случаями, когда хакеры устанавливали веб-оболочки, и их число растет с каждым часом.

Компании варьируются от финансовых учреждений, до производства и розничной торговли.

Шон Тикл, глава CyberGuard, сказал: «Это широко распространенный случай, когда хакеры направляют свои атаки на как можно больше целей, прежде чем компании смогут защитить свои системы.

«Достаточно лишь кому-то изменить этот подход, чтобы избавиться от более вредоносного пакета вредоносных программ, и мы увидим реальный ущерб для компаний, которые отстают.

«Уже ходят слухи о том, что эти оболочки используются, и я думаю, что мы увидим массовые атаки программ-вымогателей как вторую волну». ***(Joe Tidy. Exchange email hack: Hundreds of UK firms compromised // BBC (https://www.bbc.com/news/technology-56365372). 12.03.2021).***

***

«Как сообщили во вторник HP и Bromium, злоумышленники в Интернете использовали электронную почту в качестве основного средства доставки вредоносного ПО своим жертвам в последнем квартале 2020 года.

Отчет HP-Bromium Threat Insights Report показал, что 88 процентов вредоносных программ было доставлено по электронной почте в почтовые ящики его целей, что во многих случаях обходилось без мер на почтовых шлюзах по фильтрации зараженной корреспонденции.

«В конечном итоге злоумышленники пользуются тем фактом, что обмен и открытие документов по электронной почте - это нормально», - заметил Алекс Холланд, старший аналитик вредоносных программ в HP.

«Финансовые и ИТ-отделы, как правило, активно используют макросы для автоматизации бизнес-процессов, поэтому запретить их повсеместно часто нереально», - сказал он TechNewsWorld.

Электронная почта по-прежнему будет основным средством доставки из-за слабости вовлеченных в нее людей, утверждает Джозеф Нойманн, директор по безопасности в Coalfire, провайдере консультационных услуг по кибербезопасности из Вестминстера, штат Колорадо.

«В отличие от брандмауэров или серверов, уровень осведомленности о безопасности у каждого человека разный и меняется ежечасно в зависимости от того, сколько кофе он пил или не пил», - сказал он TechNewsWorld.

Двир Саяг, руководитель отдела исследований киберугроз в Hunters, открытой компании по поиску угроз XDR с офисами в Тель-Авиве и Лексингтоне, штат Массачусетс, добавил, что хакеры понимают, что фишинговые атаки по электронной почте, особенно с использованием социальной инженерии, являются одними из самых экономически эффективных способов защиты.

«Макросы Word легко купить или написать код с нуля, а заставить жертву щелкнуть по одному из них с помощью простой атаки по электронной почте с помощью социальной инженерии, в большинстве случаев не требует усилий», - сказал он TechNewsWorld.

Обнаружение уклонения

В отчете HP-Bromium отмечено увеличение на 12 процентов по сравнению с предыдущим кварталом использования вредоносных программ, которые использовали уязвимость, используемую для запуска вредоносных сценариев при открытии документа Microsoft Word.

Исследователи HP также обнаружили на 12% рост использования вредоносных исполняемых файлов, при этом почти три четверти из них используют уязвимость повреждения памяти в редакторе формул Microsoft Office.

«Основное преимущество исполняемого файла состоит в том, что вы устраняете необходимость в промежуточных этапах вредоносного ПО и размещении полезной нагрузки, которые могут быть отключены регистраторами доменов и веб-хостами», - пояснил Холланд.

В отчете HP также указано, что среднее время, в течение которого антивирусные механизмы узнают об угрозах с помощью хеширования, составляло более недели (8,8 дней).

«Угрозы занимают так много времени из-за способности вредоносных программ изменять сигнатуры», - пояснил Нойман.

«AV-хеши должны быть сгенерированы кем-то, кто идентифицирует вредоносное ПО и затем отправляет его как плохое», - продолжил он. «AV-обнаружения, основанные только на хеш-значениях, - это умирающее животное, и их все чаще заменяют системами, которые обнаруживают и реагируют на эвристические поведенческие обнаружения»…

Методы запутывания

Исследователи HP также сообщили, что 29% вредоносных программ, захваченных для анализа, ранее были неизвестны, в первую очередь из-за широкого использования упаковщиков и методов обфускации, используемых для уклонения от обнаружения…

«Проблема с «ранее неизвестными» угрозами заключается в том, что изначально нет известных индикаторов компрометации, что означает, что первоначальное обнаружение должно исходить от поведения злоумышленника или какой-либо другой деятельности, которая выявляет их присутствие», - сказал представитель TechNewsWorld.

Один из способов сокрытия своей деятельности злоумышленниками - использование секретных каналов, заметил Брайан Кайм, старший аналитик Forrester Research…

Методом обфускации, упомянутым в отчете HP, является DOSfuscation. Это набор техник обфускации, описанных исследователем безопасности Дэниелом Боханноном в 2018 году.

«Они предназначены для обхода жестких правил обнаружения путем сокрытия подозрительных строк в интерпретаторах командной строки и журналах», - пояснил Холланд…

Традиционные недостатки

Нойманн утверждал, что большинству хакеров не нужно скрывать свои угрозы.

«Большинство эксплойтов и техник используют общие уязвимости или используют социальную инженерию для получения доступа и разграбления сетей», - сказал он…

Глобальный руководитель отдела безопасности персональных систем HP Ян Пратт отметил, что в ежеквартальном отчете подчеркиваются недостатки традиционных средств защиты, которые полагаются на обнаружение, чтобы блокировать проникновение вредоносных программ на конечные точки…

«Изоляция приложений посредством виртуализации обеспечивает доступ с наименьшими привилегиями к рискованным действиям на конечной точке, делая вредоносные программы безвредными, изолируя их на микровиртуальных машинах», - пояснил он. «Аппаратно-принудительная изоляция исключает возможность вредоносного ПО причинить вред хост-компьютеру - даже с помощью нового вредоносного ПО - потому что оно не полагается на модель безопасности с обнаружением и защитой».

Чрезмерное инвестирование в профилактику

Пока существуют уязвимости нулевого дня, стратегии предотвращения будут иметь высокий процент отказов, утверждает Тим Уэйд, технический директор группы технического директора Vectra AI, поставщика решений для автоматического управления угрозами из Сан-Хосе, Калифорния.

«Текущее состояние организационных чрезмерных инвестиций в профилактику - это почти всегда упражнение в дорогостоящем, незначительном увеличении возможностей с удушающей стоимостью парализованных бизнес-целей и все более ограничивающейся производительностью. Что более важно, чем предотвращение, это устойчивость, которая включает в себя определение

инвестиций в безопасность, которые минимизируют воздействие атаки». ***(John P. Mello Jr. New Threat Report Finds Email Prime Vehicle for Malware // ECT News Network, Inc. (https://www.technewsworld.com/story/87056.html). 16.03.2021).***

***

«Королевскому университету в Белфасте (QUB) пришлось приостановить доступ к «ряду университетских систем» в качестве меры предосторожности после попытки кибератаки.

Однако в университете заявили, что «в настоящее время нет доказательств» кражи каких-либо данных.

Queen's также сообщила, что расследование нападения продолжается.

Агентство кибербезопасности Великобритании заявило, что оно «осведомлено» об инциденте, затронувшем Королевский университет, и «работает над полным пониманием его последствий».

Национальный центр кибербезопасности (NCSC) также заявил, что «университет уже подтвердил, что немедленное оперативное воздействие было смягчено».

NCSC ранее предупреждал о росте числа кибератак на колледжи и университеты Великобритании.

Центр выпустил предупреждение в начале 2020-2021 учебного года после всплеска нападений на образовательные учреждения.

В своем заявлении Queen's сообщила, что попытка кибератаки произошла в среду, 24 февраля.

«Университет приостановил доступ к ряду университетских систем в качестве меры предосторожности после попытки кибератаки», - говорится в сообщении.

«К сожалению, подобные атаки на крупные организации не редкость.

«В университете действуют надежные меры безопасности, которые смягчают непосредственные операционные последствия, и в настоящее время нет доказательств какой-либо кражи данных.

«Университет применил ряд мер предосторожности, включая приостановку доступа, и они были отменены, где это было возможно, после завершения соответствующих расследований».

Queen's заявила, что поддерживала связь с соответствующими органами и проводит оценку любых будущих рисков.

Будущие риски

«Университет понимает, что другие организации применяют свои собственные меры предосторожности, и поддерживает их в этом», - добавил он.

Пока не ясно, о каких организациях идет речь в университете. Тем не менее, Queen's заявила, что серьезно относится к своей ответственности по защите своих систем и данных…». ***(By Robbie Meredith & Eve Rosato. Queen's University takes 'precautions' after cyber-attack attempt // BBC (https://www.bbc.com/news/uk-northern-ireland-56287355). 05.03.2021).***

***

«Центр жалоб на Интернет-преступления ФБР опубликовал свой годовой отчет. Internet Report Criminal 2020 включает информацию от 791,790 заявителей, подозревающих о совершённых интернет-преступлениях – их число возросло на более чем 300000 жалоб по сравнению с 2019 годом - убытки превысили $ 4,2 млрд. Также были опубликованы статистические данные по штатам, которые можно найти в Internet Report Criminal 2020 и в прилагаемых к нему государственных отчетах за 2020 год.

Три основных преступления, о которых сообщили жертвы в 2020 году, - это фишинговое мошенничество, мошенничество с невыплатой / недоставкой и вымогательство. Жертвы потеряли большую часть денег из-за мошенничества, связанного с деловой электронной почтой, романтическими отношениями и доверием, а также мошенничества с инвестициями. Примечательно, что в 2020 году появились мошенники, использующие пандемию COVID-19. IC3 получил более 28500 жалоб, связанных с COVID-19, от мошенников, нацеленых как на юридических, так и на физических лиц.

В дополнение к статистическим данным, Отчет IC3 содержит информацию о наиболее распространенных интернет-мошенничествах, затрагивающих население, и предлагает рекомендации по предотвращению и защите. В нем также освещается работа ФБР по борьбе с преступностью в Интернете, включая недавние примеры. Наконец, Отчет рассказывает о IC3, его миссии и функциях.

IC3 предоставляет общественности надежный и удобный механизм для сообщения ФБР о предполагаемых преступлениях в Интернете. ФБР анализирует и передает информацию из поданных жалоб в целях расследования и разведки, для правоохранительных органов и для информирования общественности.

По словам Ванессы Пегерос, директора по доверительному управлению и безопасности OneLogin, «киберпреступники мастерски умеют играть на человеческих эмоциях. Они пользуются человеческим одиночеством, опасениями по поводу здоровья и отчаянными надеждами на быструю экономическую выгоду. Компьютеры не обладают эмоциями и являются средством, с помощью которого киберпреступники монетизируют эти человеческие эмоции. Нам нужно продолжать внедрять меры безопасности на компьютерах, потому что мы не изменим нашу человечность».

Джером Бекварт, главный операционный директор, Axiad, объясняет: «Фишинг электронной почты остается растущей проблемой, потому что самая большая уязвимость организации - ее пользователи. Несмотря на все усилия компаний по обучению пользователей распознаванию фишинговых писем и внедрение все более умных решений для фильтрации электронной почты, хакеры по-прежнему находят новые способы обмануть пользователей и пройти через систему. В большинстве случаев мошенничество с электронной почтой маскируется под известного источника электронной почты или коллег в той же организации, что увеличивает вероятность того, что получатель поделится конфиденциальной информацией. Для предотвращения этого следует шире использовать цифровую подпись электронных писем, поскольку они позволяют получателю электронной почты подтвердить, что отправитель является подлинным

и законным. По нашему опыту в Axiad, внедрение цифровой подписи для электронной почты значительно снизило риск фишинга по электронной почте,

«Проблема с взломом учетных данных пользователя не является новой проблемой - пароли небезопасны и являются легкой мишенью для мошенников и хакеров, что является одной из причин, по которым проблемы с учетными данными составляют более 80% утечек данных. Хорошая новость заключается в том, что мы видим, что многие организации переходят на беспарольный подход с использованием таких технологий, как FIDO2 и PKI. Эти технологии широко доступны и поддерживаются всеми основными игроками, от Microsoft до Google и AWS. Эти подходы приводят не только к лучшей безопасности, но и к лучшему взаимодействию с пользователем, так как пароли сложно запоминать, их нужно часто менять и т. д. Однако для предприятий важно развертывать беспарольные решения для различных бизнес-сценариев, таких как FIDO2 или PKI». ***(FBI releases the Internet Crime Complaint Center 2020 Internet Crime Report // BNP Media (https://www.securitymagazine.com/articles/94842-fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report). 18.03.2021).***

***

«Финансовая кибербанда проводит ограниченные атаки перед более широкими атаками на системы торговых точек.

Исследователи обнаружили, что группа кибератак FIN8 вновь появилась после периода относительного затишья. Банда использует новые версии бэкдора BadHatch для компрометации компаний в сфере химического страхования, розничной торговли и высоких технологий.

Согласно анализу Bitdefender… атаки были замечены в организациях по всему миру, в основном в Канаде, Италии, Панаме, Пуэрто-Рико, Южной Африке и США.

FIN8 - это финансово мотивированная группа угроз, типичным способом атаки которой является кража данных платежных карт из точек продаж (PoS), особенно в розничных магазинах, ресторанах и гостиничном бизнесе. Группа активна как минимум с 2016 года, но ее деятельность характеризуется периодами бездействия.

В данном случае, по словам Богдана Ботезату, директора по исследованиям угроз Bitdefender, в последний раз FIN8 поражал цели в середине 2019 года.

«Они бездействовали в течение 18 месяцев (они произвели большой всплеск в 2017 и 2019 годах), хотя они проводили тесты на небольших пулах целей», - сказал он Threatpost.

FIN8 тестирует воду с ограниченными атаками

На данный момент Bitdefender идентифицировал конкретные атаки на семь целей в ходе мониторинга инфраструктуры командного центра, используемой в предыдущих атаках FIN8.

«Хотя это может показаться незначительным, FIN8, как известно, возвращается в бизнес с небольшими тестами на ограниченном круге жертв, прежде чем они станут общими», - сказал Ботезату Threatpost. «Это механизм для

проверки безопасности на небольшом подмножестве перед переносом атак в производственную среду».

Он добавил, что в 2020 году наблюдались и другие очаги ограниченного тестирования.

Такой экспериментально-программный подход обычно истекает из групповой доработки или пополнения своего арсенала оружия. И действительно, последняя волна активности включает новую версию бэкдора BadHatch.

В течение 2020 года и в этом году было проведено три различных кампании «ограниченного выпуска» с использованием обновленных версий BadHatch.

«Переход от устаревшей версии 2.12 к текущей версии 2.14 начался в середине 2020 года (версия 2.14 была развернута во время Рождества 2020 года)», - сказал Ботезату.

Развитие вредоносного ПО BadHatch

BadHatch - это специальная вредоносная программа FIN8, которая также использовалась в атаках 2019 года… он был усилен, с заметными улучшениями в устойчивости, шифровании, сборе информации и способности выполнять боковое движение.

Последняя версия бэкдора (v. 2.14), например, злоупотребляет sslip.io - службой, которая обеспечивает бесплатное сопоставление IP-адресов с доменами, чтобы упростить создание сертификатов SSL. BatchHatch использует шифрование для сокрытия команд PowerShell во время передачи. По словам Ботезату, хотя сервис является законным и широко используется, вредоносное ПО злоупотребляет им, пытаясь избежать обнаружения.

«Это предотвращает идентификацию и блокировку скриптов PowerShell во время доставки с командно-административного сервера (C2) с помощью решений безопасности и некоторых решений для мониторинга», - сказал он. «Это особенно важно для достижения скрытности и, в большей степени, настойчивости».

Вредоносная программа также добавила к своим возможностям отслеживания, с возможностью узнать больше о сети жертвы, например, путем захвата снимков экрана - это в конечном итоге лучше позволяет горизонтальное перемещение в среде организации.

«Боковое перемещение имеет решающее значение, поскольку оно нацелено на POS-сети», - пояснил Ботезату. «Это связано с тем, что вредоносное ПО обычно доставляется через вредоносные вложения. Целевая жертва может быть кем угодно в сети, и вредоносная программа должна переходить с одной конечной точки на другую, пока не достигнет реальных целей в сети - POS-устройств».

Последняя версия BadHatch также позволяет скачивать файлы, что может подготовить почву для различных атак в будущем, помимо сбора данных с кредитных карт.

«BadHatch всегда ассоциировался с POS-атаками, но он имеет расширенные возможности бэкдора, которые позволяют операторам выполнять боковое перемещение, а также имеет возможность загружать дополнительные полезные данные из определенных мест», - сказал Ботезату. «Эти полезные данные могут играть несколько ролей в зависимости от намерений злоумышленников».

Как и большинство настойчивых и опытных участников киберпреступности, операторы FIN8 постоянно совершенствуют свои инструменты и тактику, но они все же попадают в предсказуемый ритм. По словам исследователя, последняя активность указывает на то, что в ближайшее время можно ожидать более широких атак.

«FIN8 - это высшие хищники экосистемы финансового мошенничества», - сказал Ботезату. «Они делают длительные перерывы, чтобы усовершенствовать свои инструменты, и вкладывают значительные ресурсы в обход традиционных ситуаций с безопасностью. Они чрезвычайно сосредоточены на атаках «живя за счет земли» и начинают нацеливаться на жертв только после того, как они проверили свои инструменты в бою» ***(Tara Seals. FIN8 Resurfaces with Revamped Backdoor Malware // Threatpost (https://threatpost.com/fin8-resurfaces-backdoor-malware/164684/). 11.03.2021).***

***

«Университет Высокогорья и островов (UHI) в Шотландии парирует «продолжающийся киберинцидент», в результате которого его кампусы были закрыты.

Вчера днем в послании студентам и сотрудникам учреждение, расположенное в 13 местах в самой северной части Великобритании, предупредило, что пострадали «большинство услуг», включая виртуальную среду обучения Brightspace…

В электронном письме, отправленном студентам и опубликованном на веб-сайте UHI, говорилось, что его Office 365, Cisco Webex, OneDrive, Teams и почтовые службы, среди прочего, не пострадали от очевидного вторжения. Администраторы подтвердили, что не верят, что личные данные были затронуты…

Постоянные читатели узнают, что формулировка UHI имеет много общего с ранними стадиями предыдущих атак с использованием программ-вымогателей: неустановленные «киберинциденты», которые таинственным образом нарушают работу большого количества ИТ-сервисов в организации, являются обычным сигналом. Подобные инциденты происходили со страховыми компаниями, благотворительными организациями и другими корпоративными (и образовательными) организациями все чаще и чаще за последний год…». ***(Gareth Corfield. University of the Highlands and Islands shuts down campuses as it deals with 'ongoing cyber incident' // The Register (https://www.theregister.com/2021/03/08/uni_highlands_islands_cyber_incident/). 08.03.2021).***

***

«Мошенники по компрометации деловой электронной почты (BEC) используют новый тип атак, нацеленных на инвесторов, которые могут увеличить выплаты в семь раз больше, чем в среднем.

Когда инвестор совершает покупку в инвестиционный фонд фирмы, такой как фонд прямых инвестиций или фонд недвижимости, фирма может попросить инвестора сохранить деньги до тех пор, пока они не потребуют их. Это соглашение

позволяет инвестору хранить свои деньги в более выгодных инвестициях для получения процентов, а не сидеть сложа руки в инвестиционном фонде, и фонд может потребовать инвестиции, когда это необходимо.

Когда инвестиционный фонд готов использовать деньги инвестора, он выпускает уведомление о требовании капиталовложений, формальное требование к инвестору отправить им согласованные деньги.

Мошенники BEC нацелены на Уолл-стрит

В новом отчете компании Agari, занимающейся кибербезопасностью электронной почты, мошенники BEC начали нацеливаться на инвесторов с помощью фальшивых уведомлений о требовании капиталовложений, которые несут гораздо большие выплаты, чем ваше стандартное мошенничество с BEC.

В опубликованном сегодня отчете «Тенденции мошенничества с электронной почтой и обмана идентификационной информации в 2021 году» Agari заявляет, что средняя целевая выплата при мошенничестве с использованием электронного перевода BEC составляет 72000 долларов. Это мошенничество, когда злоумышленники выдают себя за продавца и просят жертву отправлять платежи на банковский счет, находящийся под их контролем.

Поскольку фальшивые уведомления о вызове капитала имеют среднюю целевую выплату в размере 809 000 долларов, что в семь раз больше, чем обычная афера с банковским переводом, злоумышленники начинают использовать их в надежде на гораздо более крупную выплату.

"В электронных письмах к целям участники BEC маскируются под фирму, запрашивающую перевод средств в соответствии с инвестиционным обязательством. Из-за характера таких транзакций запрашиваемые платежи значительно выше, чем запрашиваемые при большинстве мошеннических операций с электронными переводами. Средняя выплата в рамках схем привлечения капитала: 809 000 долларов ", - поясняет Агари в своем отчете.

По словам Агари, атаки инициируются злоумышленниками, которые рассылают по электронной почте специалистам по кредиторской задолженности известных инвесторов с уведомлениями о вызове капитала с просьбой об оплате фиктивных инвестиций.

«Исходя из того, что мы видели, злоумышленники не используют какие-либо инсайдерские знания в своих атаках, запрашивая платежи по вызову капитала. Напротив, атаки запрашивают платежи за фиктивные инвестиции, аналогично тому, что мы видели в течение многих лет, когда субъекты BEC запрашивают платежи фиктивным поставщикам», - сказал BleepingComputer Крейн Хассолд, старший директор Agari по исследованию угроз.

Хассольд объяснил, что атаки, обнаруженные Agari, отправляются из почтовых служб, чаще всего от провайдера веб-почты centrum.cz, базирующегося в Чешской Республике.

К этим электронным письмам прилагается документ, олицетворяющий уведомление о вызове капиталов и требующий оплаты поддельных инвестиций.

Если им удастся убедить цель перевести деньги, злоумышленники быстро переведут деньги на другие счета, находящиеся под их контролем, и используют денежных мулов для снятия денег, чтобы банк не мог вернуть их жертве.

В то время как мошенничество с электронным переводом никуда не денется, злоумышленники, выполняя различные атаки в зависимости от конкретной жертвы, могут получить гораздо большие выплаты.

Чтобы защититься от таких атак, как инвестиционные фирмы, так и инвесторы должны использовать надежную защиту электронной почты…». ***(Lawrence Abrams. Investors are the next target of large-scale cyberattacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/investors-are-the-next-target-of-large-scale-cyberattacks/). 03.03.2021).***

***

«Форум по киберпреступности Maza был взломан, и данные его участников просочились в ходе последней из серии атак, нацеленных в основном на русскоязычные хакерские форумы.

Maza, также известный как Mazafuka, является одним из старейших форумов киберпреступников, где остальная часть сообщества должна проголосовать за новых участников, прежде чем им будет предоставлен доступ.

«Maza считается одним из старейших и элитных криминальных сообществ с одним из самых высоких барьеров входа для хакеров со времен форума DirectConnection (дом операторов Dridex)», - сообщает компания Advanced Intel, занимающаяся разведкой кибербезопасности…

«Форум Maza взломан, и учетные данные просочились! Verified, Dread, club2crd и теперь maza, безопасны ли форумы darkweb?», - заявил пользователь Twitter вместе со следующим снимком экрана с утечкой.

Утечка данных состоит примерно из 2 982 пользовательских записей и содержит идентификаторы пользователей, имена пользователей, адреса электронной почты, отредактированные пароли, имена файлов сертификатов, пароли сертификатов и контактную информацию участников на icq, aim, yahoo, msn и skype.

В отличие от большинства форумов, Maza требует от своих участников создания сертификата и соответствующего пароля, который используется вместе с именем пользователя и паролем для входа на форум. Эта дополнительная безопасность создает более безопасную аутентификацию, при которой только те, у кого есть соответствующий сертификат, могут войти в систему.

В этой утечке также были раскрыты пароли сертификатов членов Maza, но не сами сертификаты.

Хотя не все поля содержали контактную информацию, в некоторых учетных записях были указаны учетные записи ICQ, которые обычно используются для связи с другими злоумышленниками, что делает эту информацию ценной для правоохранительных органов.

Русскоязычные хакерские форумы атакованы

Maza - не единственный русскоязычный хакерский форум, подвергшийся недавним атакам.

Человек, который вчера вечером поделился утечкой Maza с BleepingComputer, также поделился скриншотами сообщений, сделанных в Verified, Dread и Club2Crd о недавних атаках на их форумах.

Согласно Flashpoint, то сообщество киберпреступников решительно берется с неизвестными операторами, которые утверждали, что используют уязвимость, чтобы взять под свой контроль сайт.

Снимок экрана, предоставленный BleepingComputer, предназначен для сообщения, в котором новый оператор объясняет, как они захватили форумы и свои планы относительно сайта.

Днем позже «мак», сотрудник форума по кардингу и киберпреступности «Club2Crd», объявил, что его учетная запись Club2Crd была взломана с целью мошенничества на сайте и кражи денег у других участников.

«Кроме того, у одного из старейших супер-модераторов форума среднего уровня Club2Crd «mak» произошел полный захват аккаунта, в результате чего появилось множество новых мошеннических сервисов и снизилось доверие к сообществам киберпреступников», - пояснил Кремез BleepingComputer.

Наконец, похожий на Reddit темный веб-сайт Dread подвергся атакам в феврале примерно в то же время, что побудило их ввести новые защитные меры для предотвращения будущих кибератак.

Неизвестно, является ли человек, связавшийся с BleepingComputer, тем, кто атаковал эти форумы, или просто является их участником.

Однако эти атаки показывают, что от кибератак никто не застрахован, в том числе и сами хакеры». ***(Lawrence Abrams. Notorious Maza cybercrime forum attacked by other hackers // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/notorious-maza-cybercrime-forum-attacked-by-other-hackers/). 04.03.2021).***

***

«Сайт разработчиков известного ПО, которым пользуются множество организаций по всему миру, частично не функционировал в течение многих часов из-за попытки его взлома. Атака оказалась безуспешной, но не исключены рецидивы.

Атака на Blender

Разработчикам пакета для создания компьютерной графики Blender 15 марта 2021 г. пришлось частично отключить основной сайт Blender.org для проведения технических работ после попытки кибератаки на него. Речь идет только о сайте и некоторых связанных с ним блогах; техническая инфраструктура, Wiki, портал разработчиков, git-репозитории и ресурс Blender Cloud атака не затронула.

Ночью 16 марта функциональность сайта была восстановлена в полном объеме. Кому и зачем понадобилось атаковать его, не известно. В соцсетях тиражируются конспирологические версии о «конкурентах, которым Blender очень мешает», но подтверждений им пока нет.

Blender является очень популярным пакетом у энтузиастов 3D-графики в силу своей бесплатности, однако его зрелость и функциональность действительно позволяют ему всерьез конкурировать с коммерческими разработками, такими как Maya и 3dsMax. Это привело к росту популярности Blender и в профессиональной среде — в диапазоне от отдельных фрилансеров до бюджетных студий и академических организаций (включая, например, учреждения Российской академии

наук). Вдобавок Blender — опенсорсная разработка с большим потенциалом к расширяемости, так что образовавшаяся вокруг него экосистема уже весьма велика.

Все это делает его весьма интересной мишенью для киберзлоумышленников, нацелившихся на сети компаний, пользующихся данным софтом.

Атаки на цепочки поставок

Атаки на крупные компании через подрядчиков или цепочки поставок — довольно распространенное явление. Одним из самых драматичных примеров последнего времени стала атака на мониторинговое ПО Orion, которое производит компания SolarWinds. Скомпрометировав систему сборки и развертывания Orion, киберзлоумышленники смогли в конце 2020 г. проникнуть в сети бесчисленного количества коммерческих компаний (включая поставщиков средств информационной безопасности) и множества госорганов в США, получив доступ к конфиденциальной, а то и секретной информации.

Позднее стало известно, что некая кибергруппировка на протяжении нескольких лет эксплуатировала другую платформу мониторинга, разработку французской компании Centreon, для атак на хостинг-провайдеров. И это тоже было типичной атакой через цепочку поставок.

До недавнего времени Blender или связанные с ним ресурсы нечасто становились объектами кибератак, во всяком случае таких, о которых становилось известно публично. Несколько раз были отмечены атаки на сторонние сайты, связанные с сообществом пользователей Blender, но не на основной сайт.

Пока можно констатировать, что атака на Blender.org успешно отбита. Администраторы сайта проверили контрольные сигнатуры всего, что выложено на сайте, и пока что злоумышленникам не удалось ничего скомпрометировать. Однако чем более популярен тот или иной пакет, тем больше вероятности, что кто-то попытается воспользоваться им для причинения вреда другим.

«Хотя конкретной информации о кибератаке мало, логично предположить, что целью злоумышленников было скомпрометировать дистрибутивы Blender, выложенные на официальном сайте, причем не обязательно самые последние, — полагает Анастасия Мельникова, эксперт по информационной безопасности компании SEC Consult Services. — В силу своей популярности Blender представляет собой неплохую мишень для атаки через “цепочки поставок”: дистрибутив со встроенным в него вредоносным компонентом вполне может обеспечить злоумышленников точками входа в инфраструктуру множества организаций — никто не ожидает от 3D-пакета, что он станет источником кибератаки». ***(Роман Георгиев. Хакеры сломали сайт сверхпопулярного 3D-пакета, лишив доступа к нему компании по всему миру // CNew (https://safe.cnews.ru/news/top/2021-03-17_hakery_slomali_sajt_sverhpopulyarnogo). 17.03.2021).***

***

«В фальшивом заявлении говорилось, что здоровье граждан, проживающих возле литовской границы, якобы находится в опасности из-за утечки ядерных отходов.

Web-сайты правительства Польши были взломаны киберпреступниками с целью распространения ложной информации о несуществующей радиоактивной угрозе. Об этом сообщило информагентство Associated Press.

На сайтах Национального агентства по атомной энергии и Министерства здравоохранения Польши были опубликованы сообщения о предполагаемой утечке ядерных отходов в Литве, угрожающей Польше.

Кроме того, был взломан Twitter-аккаунт журналиста, который часто пишет о России и странах Восточной Европы. Учетная запись использовалась для дальнейшего распространения информации.

Пресс-секретарь главы службы безопасности Польши Станислав Зарин сообщил, что «вся эта история выглядит как типичная попытка России» посеять подозрения и раскол среди западных союзников…». ***(Сайты польских ведомств взломали для распространения фейков // SecurityLab.ru (https://www.securitylab.ru/news/517570.php). 18.03.2021).***

***

«Главные вызовы для кибербезопасности в этом году будут связаны с новыми вирусами в электронных письмах, продуманными фишинговыми кампаниями, слабо защищенными конечными устройствами, на которых люди работают из дома, а также ростом популярности электронной коммерции.

В 2020 году Tet (ранее Lattelecom) предотвратил 2400 DDoS-атак, а также заблокировал 140 тысяч вредоносных писем, что на 50% больше, чем годом ранее.

«Глядя на статистику 2020 года, мы видим, что пандемия отразилась и на киберпространстве, поскольку выросло как число вирусов, так и нападений. Согласно данным Tet, самым популярным для DDoS-атак периодом стал второй квартал 2020 года, в который начался массовый переход на работу из дома. В третьем и четвертом кварталах киберпреступники сфокусировались на нападениях, направленных против финансовых учреждений и критической инфраструктуры государств», — говорит управляющий ИТ-безопасностью Tet Улдис Либиетис.

По данным аналитиков Tet, DDoS-атаки теперь длятся еще дольше — если ранее они занимали десятки минут, то теперь хакеры могут атаковать компанию несколько часов, а затем повторить нападение. В связи с ростом популярности электронной коммерции и цифровых технологий в целом, тенденция на усложнение DDoS-атак продолжится и в этом году.

«Управление несколькими потоками данных, размером более 100 Гбит/с с небольшими перерывами на протяжении нескольких дней, нереально организовать одному человеку или небольшому кругу лиц. Такие действия целенаправленно координируются. Остается лишь гадать, кто на самом деле заказывает и планирует подобные атаки. Одно ясно точно — в этом году они никуда не исчезнут», — делится Улдис.

Еще одна заметная тенденция — скомпрометированное программное обеспечение. Сегодня от таких типов атак страдают и ИТ-гиганты.

«Современные ИТ-решения нередко имеют в своей основе ПО, написанное третьими лицами и состоящее из продуктов многих небольших разработчиков или

открытого кода. Хакеры пользуются этим, чтобы попасть в крупные системы с помощью малых звеньев в цепочке создания решения. Мы ожидаем увеличение подобных инцидентов в 2021 году», — рассказывает Улдис.

Похожая ситуация уже произошла в 2020 году с Solarwinds Orion, когда многие компании, в том числе Microsoft и VMware стали жертвами, используя ПО от надежного производителя, которое оказалось скомпрометированным. В первую очередь это говорит о том, что организациям, которые сами занимаются разработкой, придется внедрять новые или кардинально менять существующие процессы для контроля компонентов ПО и процесса разработки.

До сих пор актуальной остается проблема зараженных электронных писем. С августа 2020 года специалисты Tet по информационной безопасности наблюдают стремительный рост вирусной активности — количество вредоносных файлов в электронных письмах выросло почти вдвое (до 140 000). Особого внимания в последние годы заслуживал вирус Emotet, остановить деятельность которого удалось в начале 2021 года благодаря скоординированной работе сразу нескольких государств.

Тревожная тенденция наблюдается с распространением вирусов через файлы формата .edoc и .asice, которые люди открывают, несмотря на предупреждения антивируса. Также эксперты Tet фиксируют все более продуманные фишинговые кампании. Переводчик Google и подобные работает все лучше, благодаря чему нападающие за границей могут создавать все более качественные и убедительные письма и рекламу на русском языке.

Исходя из данных прошлого года, а также видя, как развивается ситуация с пандемией и ее последствиям во всем мире, уже сейчас понятно, что в фокусе кибермошенников находится конечный пользователь и его устройства.

«Зачем пытаться взломать периметр безопасности предприятия, файрволл или хорошо защищенное облако, если вместо этого можно сфокусироваться на самом слабо защищенном звене — человеке? Старое ПО, отсутствие защиты от вирусов, наличие прав администратора, ограниченные возможности контроля сотрудников или вообще его отсутствие делают работников легкой мишенью. Для защиты против угроз придется улучшить как знания работников, так и внедрить новые решения по безопасности», — добавляет Улдис». ***(Вызовы для кибербезопасности в 2021: более мощные DDoS-атаки, новые вирусы и уязвимые к ним устройства // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5723399-Vyzovy-dlya-kiberbezopasnosti-v-202.html). 10.03.2021).***

***

«Представители IT-отрасли во всем мире на фоне пандемии и связанных с ней финансовых сложностей резко увеличили предложение работы в даркнете и на хакерских форумах. Как правило хакеры сами размещают вакансии, но теперь ситуация изменилась: люди сами готовы работать на кибермошенников, сообщил глава стартап-проекта ScorCool Павел Педина.

"Теперь это может стать большой проблемой для всех. Соискатели предлагают свои услуги по обналичиванию денег, готовы стать "отправителями",

рейдерами и курьерами. Теперь людям и компаниям стоит быть еще более внимательными. Как известно, спрос рождает предложения", – отметил бизнесмен.

Педина приводит свежий пример, когда испанские фальшивомонетчики, среди которых задержали 37 человек, изготовляли поддельные купюры номиналом €500. При обысках были изъяты фальшивые банкноты на общую сумму в €201 тыс., €12 тыс. в биткоинах и €32 тыс. настоящих денег.

"В Барселоне задержаны несколько человек – уроженцев Румынии. За денежное вознаграждение они должны были открывать банковские счета на свое имя и пополнять их через терминалы фальшивыми купюрами. Задержанным предъявлены обвинения в изготовлении фальшивых купюр, мошенничестве, подделке документов, отмывании денег", – рассказал он…». ***(Максим Беркаль. Айтишники начали массово проситься на хакерские форумы в поисках работы // UBR.UA (https://ubr.ua/ukraine-and-world/technology/ajtishniki-nachali-massovo-prositsja-na-khakerskie-forumy-v-poiskakh-raboty-4000733). 24.03.2021).***

***

«87% организаций в мире столкнулись с попыткой использования уже известной уязвимости, а в 46% организаций хотя бы один сотрудник загрузил вредоносное мобильное приложение.

Команда исследователей Check Point Research, подразделение Check Point Software Technologies, опубликовала отчет Cyber Security Report 2021. Отчет показывает, какие инструменты и методы использовали киберпреступники в 2020 году для атак на организации по всему миру. Cyber Security Report предоставляет специалистам по кибербезопасности и руководителям компаний информацию, необходимую для защиты организаций от текущих кибератак и угроз Пятого поколения.

Главное в отчете 2021 Security Report:

Внедрение облаков опережает обеспечение их безопасности. Когда мы говорим о цифровой трансформации организаций, то в 2020 году компании из-за пандемии за год сделали то, что планировалось сделать в течение 5 лет. Но безопасность общедоступных облаков по-прежнему является серьезной проблемой для 75% компаний. Кроме того, более 80% предприятий обнаружили, что их существующие инструменты безопасности или вообще не работают, или имеют ограниченные возможности в облаке. Это значит, что проблемы с облачной безопасностью сохранятся и в 2021 году.

Цель – дистанционная работа: хакеры активизировали атаки типа «перехват цепочки писем». Они нацелены на удаленных сотрудников для кражи данных или проникновения в сеть с помощью троянов Emotet и Qbot. Всего эти вредоносные программы затронули 24% организаций по всему миру. Также резко возросло количество атак на системы удаленного доступа, такие как RDP и VPN.

Рост числа атак с двойным вымогательством: в третьем квартале 2020 года почти половина всех инцидентов с использованием программ-вымогателей связана с угрозой раскрытия украденных данных. В среднем каждые 10 секунд по всему миру какая-то организация становится жертвой вымогателей.

Атаки на сектор здравоохранения превратились в эпидемию: в четвертом квартале 2020 года CPR сообщил, что кибератаки (особенно атаки программ-вымогателей) на больницы во всем мире увеличились на 45%. Преступники считают, что госпитали с большей вероятностью будут удовлетворять требования выкупа из-за давления с информацией о случаях COVID -19.

Мобильные устройства – желанные цели: в 2020 году в 46% организаций по крайней мере один сотрудник загрузил вредоносное мобильное приложение, которое угрожает сетям и данным компании. Широкое использование смартфонов во время локдауна по всему миру привело к росту числа мобильных троянцев, которые атакуют мобильный банкинг и воруют информацию.

«Компании во всем мире удивили себя скоростью внедрений цифровых инициатив в 2020 году: по оценкам, цифровая трансформация продвинулась вперед на семь лет. Но киберпреступники тоже изменили свои методы, чтобы воспользоваться этими изменениями и последствиями пандемии, – рассказывает Дорит Дор, вице-президент по продуктам Check Point Software. – Мы должны действовать сейчас, чтобы остановить бесконтрольное распространение киберпандемии. Организациям необходимо вакцинировать свои сети, чтобы предотвратить кибератаки, которые вызывают столько разрушений». ***(Каждые 10 секунд в мире одна организация становится жертвой вымогателей // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5722275-Kazhdye-10-sekund-po-vsemu-miru-odn.html). 02.03.2021).***

***

«Вторая половина 2020 года продемонстрировала беспрецедентные изменения ландшафта киберугроз: злоумышленники максимально увеличивают площадь атак, чтобы масштабировать угрозы по всему миру. Противники оказались очень гибкими, создавая волны разрушительных и изощренных атак.

Атаки нацелены на большое количество удаленных сотрудников или учащихся за пределами традиционной сети. Такие выводы приведены в новом полугодовом исследовании FortiGuard Labs Global Threat Landscape Report, подготовленном компанией Fortinet.

Кроме того, говорится в отчете, киберугрозы продемонстрировали впечатляющую гибкость в попытках нацеливаться на цифровые цепочки поставок и даже базовую сеть.

Главное из отчета за II полугодие 2020 года:

Натиск программ-вымогателей продолжается: данные FortiGuard Labs показывают семикратное увеличение общей активности программ-вымогателей по сравнению с первым полугодием 2020 года, причем рост активности обусловлен несколькими тенденциями. Условия для такого интенсивного роста создают следующие факторы: развитие RaaS (программа-вымогатель как услуга), упор на большие выкупы за крупные цели и угроза раскрытия украденных данных в случае невыполнения требований. Кроме того, с разной степенью распространенности наиболее активными из отслеживаемых типов вымогателей были Egregor, Ryuk, Conti, Thanos, Ragnar, WastedLocker, Phobos/EKING и BazarLoader. Секторы

экономики, которые подвергались серьезным атакам программ-вымогателей, включают здравоохранение, сфера услуг, госсектор, финансовые организации. Чтобы эффективно бороться с растущим рисками, связанными с данным типом вредоносов, необходимо обеспечить своевременное, полное и безопасное резервное копирование данных за пределами корпоративной сети. Также, чтобы минимизировать риск, следует изучить стратегии доступа с нулевым доверием и сегментации, чтобы минимизировать риск.

Цепочка поставок в центре внимания: атаки на цепочки поставок имеют долгую историю, но случай с SolarWinds поднял дискуссию на новый уровень. По мере развития атаки затронутые организации обменивались значительным объемом информации. FortiGuard Labs внимательно следила за этой новой информацией, используя ее для создания IoCs для обнаружения связанной активности. Обнаружение связи с интернет-инфраструктурой, аффилированной с SUNBURST в декабре 2020 года, демонстрирует, что кампания была действительно глобальной по своему характеру, а «Five Eyes» демонстрировала особенно высокие показатели трафика, соответствующего вредоносным IoCs. Есть также свидетельства возможных вторичных целей, которые подчеркивают взаимосвязанный масштаб современных атак на цепочки поставок и важность управления рисками в цепочке поставок.

Злоумышленники нацелены на ваши действия в Интернете: изучение наиболее распространенных категорий вредоносных программ позволяет выявить самые популярные методы, используемые киберпреступниками для закрепления своих позиций в организациях. Главной целью атак были платформы Microsoft, связанные с документами, которые большинство людей используют в течение обычного рабочего дня. Веб-браузеры продолжали оставаться еще одним фронтом. В эту категорию HTML входили фишинговые сайты и скрипты, содержащие вредоносные программы, которые вводят скрытый код или перенаправляют пользователей на вредоносные сайты. Эти типы угроз неизбежно растут во время глобальных проблем или периодов интенсивной онлайн-торговли. Сотрудники, которые обычно пользуются услугами веб-фильтрации при просмотре из корпоративной сети, продолжают оставаться более уязвимыми, когда делают это за пределами такого защитного фильтра.

Домашний офис остается под прицелом: барьеры между домом и офисом значительно разрушились в 2020 году, а это означает, что нацеливание на дом приближает злоумышленников на один шаг к корпоративной сети. Во второй половине 2020 года эксплойты, направленные на устройства Интернета вещей (IoT), такие как те, которые существуют во многих домах, были в верхней части списка распространенных вредоносов. Каждое устройство IoT представляет собой новую «границу» сети, которую необходимо защищать и мониторить.

Злоумышленники выходят на глобальный уровень: группы Advanced Persistent Threat (APT) продолжают различными способами использовать пандемию COVID-19. Наиболее распространенными среди них были атаки, направленные на массовый сбор личной информации, кражу интеллектуальной собственности и сбор разведданных, соответствующих национальным приоритетам APT-группы. По мере приближения конца 2020 года наблюдался рост активности APT, нацеленной на

организации, участвующие в работе, связанной с COVID-19, включая исследования вакцин и разработку внутренней или международной политики здравоохранения в отношении пандемии. Целевые организации включали правительственные учреждения, фармацевтические фирмы, университеты и медицинские исследовательские фирмы.

Сглаживание кривой эксплойтов уязвимостей: патчи и исправления являются постоянными приоритетами для организаций, поскольку киберпреступники продолжают попытки использовать уязвимости в своих интересах. Данные демонстрируют, насколько быстро и насколько далеко распространяются эксплойты (на основе анализа развития 1500 эксплойтов за последние два года). Хотя это не всегда так, похоже, что большинство эксплойтов не распространяются очень быстро. Среди всех, отслеживаемых за последние два года, только 5% были обнаружены более чем в 10% организаций. При прочих равных условиях, если уязвимость выбрана случайным образом, данные показывают, что вероятность того, что организация подвергнется атаке, составляет примерно 1 из 1000. Около 6% эксплойтов поразили более 1% фирм в течение первого месяца, и даже через год 91% эксплойтов не преодолели этот порог в 1%. Тем не менее, по-прежнему разумно сосредоточить усилия по исправлению уязвимостей с известными эксплойтами, и среди них отдать приоритет тем, которые наиболее быстро распространяются в свободных условиях.

Борьба с киберпреступниками требует комплексной стратегии и широкой осведомленности

Организации сталкиваются с атаками со всех сторон. Аналитика угроз остается центральной мерой для понимания этих угроз и способов защиты от меняющихся векторов нападения. Видимость также важна, особенно когда значительное количество пользователей находится за пределами типичного сетевого сценария. Каждое устройство создает новую границу сети, которую необходимо контролировать и защищать. Использование искусственного интеллекта (ИИ) и автоматического обнаружения угроз позволит организациям реагировать на атаки немедленно, что крайне важно для снижения скорости атак и их масштабирования на всех уровнях. Обучение пользователей в области кибербезопасности также должно оставаться приоритетом, поскольку кибергигиена – это не только сфера деятельности ИТ-специалистов и команд по обеспечению безопасности. Каждому необходимо регулярное обучение и инструктаж по передовым методам для обеспечения безопасности отдельных сотрудников и все организации в целом.

«От начала и до конца 2020 года мы были свидетелями драматического развития событий в рамках ландшафта киберугроз. Хотя пандемия играла центральную роль, в течение года кибер-злоумышленники начали проводить атаки со все более разрушительными последствиями. Они максимально расширили поверхность цифровой атаки за пределами базовой сети, чтобы нацелиться на удаленную работу или обучение, а также на цифровую цепочку поставок. Риски кибербезопасности никогда не были такими большими, поскольку все взаимосвязано в более крупной цифровой среде. Интегрированные и основанные на искусственном интеллекте платформенные подходы, основанные на действенной

аналитике угроз, жизненно важны для защиты со всех сторон, а также для выявления и устранения угроз, с которыми организации сталкиваются сегодня в режиме реального времени», – комментирует Дерек Мэнки, руководитель отдела аналитики безопасности и Global Threat Alliances, FortiGuard Labs». ***(Ландшафт киберугроз радикально изменился // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5722705-Landshaft-kiberugroz-radikalno-izme.html). 04.03.2021).***

***

«Финансовые последствия кибератаки 1 марта на CompuCom, стопроцентную дочернюю компанию ODP Corporation, как ожидается, достигнут диапазона 28 миллионов долларов, говорится в сообщении компании.

После инцидента, в результате которого некоторые системы поставщика управляемых услуг были заражены вредоносным ПО, обслуживание клиентов и внутренние операции были приостановлены, но теперь ODP сообщает, что в восстановлении услуг был достигнут значительный прогресс.

Хотя никаких технических подробностей инцидента не было раскрыто, ODP утверждает, что «время простоя и связанное с этим влияние из-за инцидента с вредоносным ПО» повлияет на выручку за март, что, вероятно, повлияет на финансовые результаты за первый финансовый квартал 2021 года.

Таким образом, ODP оценивает потерю доходов в размере от 5,0 до 8,0 млн долларов США, в основном в результате временного прекращения предоставления услуг определенным клиентам.

Кроме того, компания ожидает, что связанные с инцидентом расходы составят до 20 миллионов долларов, из которых примерно 10 миллионов долларов будут начислены в течение первого квартала 2021 года.

Эти расходы, по словам ODP, связаны с усилиями по восстановлению услуг и решением «некоторых других вопросов, возникших в результате инцидента». Компания добавляет, что некоторые из этих ожиданий могут быть покрыты страховкой.

Хотя возможности доставки были существенно восстановлены к 17 марта, ожидается, что предоставление услуг для всех клиентов будет восстановлено только к концу марта 2021 года. CompuCom также предприняла шаги по усилению безопасности своих систем.

ODP предоставит дополнительную информацию о своих финансовых показателях за первый квартал во время объявления финансовой отчетности за первый квартал, которое в настоящее время запланировано на 5 мая 2021 года». ***(Ionut Arghire. CompuCom Cyber-Attack Costs Could Reach $28M // Wired Business Media (https://www.securityweek.com/compucom-cyber-attack-costs-could-reach-28m). 29.03.2021).***

***

«С тех пор, как появились первые службы мониторинга темной сети, примерно в 2005 году, потребители таких услуг часто спрашивали - почему

эти веб-сайты не закрываются? В конце концов, сайты, составляющие темную сеть, являются платформами и инструментами для незаконной деятельности.

Ответ, который раньше устраивал большинство, заключался в том, что эти сайты являются источниками разведывательной информации, и их уничтожение означает, что преступники будут собираться где-то еще, где, возможно, не знают те, кто их отслеживает.

Эти сайты являются источниками разведывательной информации как для правоохранительных органов, так и для поставщиков средств безопасности, без них будет меньше информации для предотвращения мошенничества, восстановления учетных данных и раскрытия истинной личности преступников.

Основная цель правоохранительных органов - задержать преступников, и, учитывая, что для создания доказательства требуется время, форумы в темной сети могут быть сокровищницей потенциальных клиентов и соответствующих данных для дела, которое продолжает расти по мере того, как преступники публикуют новый контент. Для них имеет смысл не трогать доску, пока они не будут готовы сделать свой ход и задержать более крупных игроков на определенном сайте, обычно это международная операция с участием нескольких местных агентств.

Для поставщиков средств безопасности это просто операционально дорого - если сайт выйдет из строя, он может вернуться в другое место в другом формате платы, что означает, что поставщику придется разрабатывать новые сканеры. В качестве альтернативы, теперь он может быть защищен новой службой обнаружения ботов, которую придется обойти или, что еще хуже, не возвращаться вообще.

Все это веские причины, подтверждающие идею о том, что мониторинг темной сети должен выполняться с минимальными нарушениями. Тем не менее, есть основания для принятия другой стратегии - максимально разрушить темную сеть - и кажется, что, в отличие от первых дней мониторинга темной сети, она вообще не обсуждается.

Так почему же, несмотря на все вышеперечисленные причины, мы должны рассмотреть возможность удаления темных веб-сайтов? Чтобы ответить на этот вопрос, нам сначала нужно поговорить о том, что такое даркнет.

Сайты в даркнете, особенно те, которые посвящены киберпреступности, состоят из трех основных типов: форумы, торговые площадки и инструменты.

Эти три типа по сути являются вариантами одного и того же - облегчения торговли товарами и услугами между преступниками. Поскольку проведение атак или мошенничества может быть сложным делом, требующим понимания в нескольких областях (например, для запуска фишинг-атаки требуется знание кодирования, получение сервера веб-хостинга, рассылка спама и т. Д.), Вместо того, чтобы изучать все самостоятельно, преступники перейдите к этим ресурсам, чтобы заполнить их пробелы. Это делается либо путем покупки недостающего инструмента, либо путем сотрудничества с кем-то другим. Другими словами, основной вклад даркнета в криминальную экосистему в целом заключается в его способности резко снизить планку доступа к киберпреступности.

Не знаете, как закодировать программу-вымогатель? Не проблема, вы можете просто купить его в даркнете у того, кто это делает. Вы хакер с доступом к

взломанным учетным данным, но не знаете, как их использовать? Не проблема, через даркнет их можно продать тем, кто это делает.

Доступ к даркнету означает возможность для многих неискушенных людей войти и участвовать в мире киберпреступности - и большинство преступников действительно таковы - технически неискушенные. Без доступа к инструментам и сервисам, предоставляемым в даркнете, они не могли бы запускать атаки самостоятельно, или им пришлось бы прибегать только к базовым, таким как 419 мошенничества.

Это движущая сила стратегии уничтожения темных веб-сайтов - они не только источники разведывательной информации для поставщиков средств безопасности и правоохранительных органов, они также источники для преступников. Уберите эти источники, и им придется либо найти другую платформу, чтобы заполнить свои пробелы, либо им придется ограничиваться только низкоуровневыми атаками, которые они знают, как полностью выполнять самостоятельно.

Есть еще один ключевой вопрос в этой дискуссии - возможно ли это вообще? Все мы знаем, что большинство темных веб-сайтов используют TOR для маскировки своего местоположения или размещаются на надежных хостингах. Можем ли мы их даже уничтожить, если захотим? Плохая новость в том, что мы никогда не сможем полностью уничтожить темную сеть или даже большую ее часть. Хорошая новость в том, что нам не нужно этого делать, чтобы увидеть положительные эффекты стратегии.

Точно так же, как обитатели даркнета различаются по сложности, сайты, являющиеся его частью, тоже различаются. Существуют форумы, которые явно предназначены только для элитных преступников в этом мире и размещаются на защищенном пуленепробиваемом хостинге, который никогда не будет выполнять какие-либо запросы на удаление. Тем не менее, существует множество форумов, которые обслуживают более начинающих мошенников. Они часто характеризуются множеством бесплатных услуг, таких как бесплатно украденные учетные данные кредитной карты, и больше подходят только для бизнеса. Эти сайты не обязательно размещаются в службах хостинга, которые будут игнорировать запросы на удаление, но вместо этого они скрыты за службами защиты от DDoS, которые скрывают IP-адрес хоста. Самые популярные анти-DDoS-сервисы - это легальные компании, расположенные в западных странах.

Речь идет не только о форумах - многие сайты в даркнете представляют собой автоматические тележки для продажи скомпрометированных учетных данных кредитных карт или скомпрометированных учетных записей. Преступники могут приобрести эти учетные данные на сайте полностью автоматически, круглосуточно. Инструменты проверки счетов и кредитных карт также широко доступны. Большинство из них не размещены на TOR, и их местонахождение может быть выяснено после расследования.

Скорее всего, применение этой стратегии приведет к новой гонке вооружений с преступниками - большинство сайтов, которые будут отключены, появятся где-то в другом месте с лучшей маскировкой местоположения, на TOR или размещены на пуленепробиваемой службе хостинга. Однако это означает, что

со временем темная сеть объединится с определенными местоположениями хостинга и методами маскирования IP-адресов, что упростит таргетинг как группу. Кроме того, нужно помнить, что когда сообщество выходит из строя, даже если оно снова появляется, оно может быть уже не таким - им придется собрать своих существующих пользователей и заставить их использовать новый сайт, что предполагает они сохранили приличную резервную копию своих данных, иначе им придется начинать все заново с нуля.

Предлагаемая стратегия - это стратегия, на которую, вероятно, не будут подписываться правоохранительные органы, которым нужно и нужно их время для расследования, или поставщики средств безопасности. Однако следует помнить, что, хотя работа правоохранительных органов важна, она никогда не встряхивала криминальную экосистему в целом, и текущая стратегия мониторинга темной сети в основном приносит пользу крупным организациям, которые могут подписаться на разведывательные службы.

Удаление темных веб-сайтов может вызвать головную боль как у плохих, так и у хороших парней, но оно также может иметь глубокий положительный эффект на борьбу с киберпреступностью в целом для всех организаций, поскольку может потребоваться множество преступников или потенциальных преступники вне уравнения». ***(Idan Aharoni. The Case for Taking Down Dark Web Sites // Wired Business Media (https://www.securityweek.com/case-taking-down-dark-web-sites). 24.03.2021).***

***

«Официальный сервер PHP Git был скомпрометирован при потенциальной попытке внедрить вредоносное ПО в кодовую базу проекта PHP.

В воскресенье разработчик и сопровождающий языка программирования PHP Никита Попов сообщил, что в репозиторий php-src были добавлены две вредоносные фиксации как на его имя, так и на имя создателя PHP Расмуса Лердорфа.

Вредоносные коммиты, которые, казалось, подписывались под именами Попова и Лердорфа (1, 2), были замаскированы под простые типографские ошибки, которые необходимо было исправить.

Однако вместо того, чтобы избежать обнаружения и выглядеть столь безобидно, участники, внимательно изучившие фиксацию «Исправить опечатку», отметили вредоносный код, который запускал произвольный код в HTTP-заголовке агента-пользователя, если строка начиналась с содержимого, связанного с Zerodium.

Как отмечает Bleeping Computer, код, по-видимому, предназначен для внедрения бэкдора и создания сценария, в котором возможно удаленное выполнение кода (RCE).

Попов сказал, что команда разработчиков не совсем уверена, как именно произошла атака, но есть свидетельства того, что скорее всего был скомпрометирован официальный сервер git.php.net, а не отдельные учетные записи Git.

В сценарий был включен комментарий «REMOVETHIS: продано Zerodium, середина 2017 года». Однако нет никаких указаний на то, что продавец эксплойта имеет какое-либо участие в кибератаке.

Генеральный директор Zerodium Чауки Бекрар назвал виновного «троллем», отметив, что «вероятно, исследователь (и), обнаруживший эту ошибку / эксплойт, пытался продать его многим организациям, но никто не хотел покупать это дерьмо, поэтому они сожгли его за веселье."

Коммиты были обнаружены и отменены до того, как они попали в нисходящий поток или затронули пользователей.

В настоящее время ведется расследование инцидента, связанного с безопасностью, и команда исследует репозиторий на предмет любых других признаков злонамеренной активности. Тем временем, однако, команда разработчиков решила, что сейчас подходящее время для постоянного перехода на GitHub.

«Мы решили, что поддержка нашей собственной инфраструктуры git представляет собой ненужную угрозу безопасности, и что мы прекратим поддержку сервера git.php.net», - сказал Попов. «Вместо этого репозитории на GitHub, которые раньше были только зеркалами, станут каноническими. Это означает, что изменения следует отправлять непосредственно на GitHub, а не на git.php.net».

Разработчикам, ранее имевшим права записи в репозитории проекта, теперь необходимо присоединиться к группе PHP на GitHub.

Инцидент безопасности можно описать как атаку цепочки поставок, при которой злоумышленники будут нацелены на проект с открытым исходным кодом, библиотеку или другой компонент, на который полагается большая база пользователей. После компрометации одной основной цели вредоносный код может проникнуть в большое количество систем.

Недавний пример - фиаско SolarWinds, когда поставщик был взломан и было установлено вредоносное обновление для его программного обеспечения Orion. После развертывания этого вредоносного ПО были скомпрометированы десятки тысяч организаций, включая Microsoft, FireEye и Mimecast». ***(Charlie Osborne. Official PHP Git server targeted in attempt to bury malware in code base // ZDNet (https://www.zdnet.com/article/official-php-git-server-targeted-in-attempt-to-bury-malware-in-code-base/). 29.03.2021).***

***

«В прошлом году взломы подверглись большему количеству организаций на шести рынках Азиатско-Тихоокеанского региона, при этом в среднем 60,83% потребовалось более недели для устранения этих атак кибербезопасности. Они называют отсутствие бюджета и навыков ключевыми проблемами и выражают разочарование по поводу очевидного отсутствия понимания того, насколько сложно управлять рисками кибербезопасности.

Около 68% респондентов в исследовании Sophos заявили, что они были успешно взломаны в прошлом году, по сравнению с 32% в 2019 году. Среди тех, кто был взломан, 55% заявили, что они понесли «очень серьезную» или

«серьезную» потерю данных, выявили Исследование, проведенное компанией Tech Research Asia, охватило 900 предприятий, в которых работает не менее 150 сотрудников, в Сингапуре, Индии, Японии, Малайзии, Австралии и на Филиппинах.

Кроме того, 17% каждую неделю сталкивались с более чем 50 кибератаками. В Сингапуре, например, почти 15% приходилось иметь дело как минимум с 50 попытками атак или ошибок в неделю. Примерно 28% в городе-государстве в конечном итоге были успешно взломаны в прошлом году, а 33% описали потерю данных как очень серьезную или серьезную.

В то время как в Сингапуре было наименьшее количество взломанных респондентов, 75% заявили, что им нужна как минимум неделя для устранения кибератаки - самый высокий показатель в регионе. Около 68% их австралийских коллег признали, что на устранение кибератак уходит больше недели, как и 65% в Индии, 64% в Малайзии, 55% на Филиппинах и 38% в Японии.

Фактически, японские организации смогли быстрее всех восстановиться после взлома: 62% потребовалось для этого меньше недели.

Респонденты по всему региону указали на вымогатели, вредоносное ПО и фишинг в качестве трех основных угроз безопасности. Они также назвали плохо спроектированные или уязвимые системы поставщиков как главный риск, который они ожидали в 2023 году, отчасти вызванный опасениями, что они могут стать целью в результате взлома сторонних уязвимостей и безопасности и других поставщиков технологий.

Около 53% признали, что они также были плохо подготовлены к требованиям безопасности, вызванным острой необходимостью поддерживать удаленную работу в условиях пандемии COVID-19. Несмотря на это, 54% компаний еще не обновили свою стратегию кибербезопасности в прошлом году, что на 3% больше, чем в 2019 году.

На вопрос, есть ли у них команда, способная обнаруживать угрозы безопасности и управлять ими, только 52% ответили положительно, по сравнению с 50% в 2019 году. Для 75% в Сингапуре пандемия стала основным стимулом для их организации к обновлению инструментов и стратегии безопасности. в прошлом году.

Исследование также показало, что респонденты были больше всего разочарованы предположениями внутри организации о том, что кибербезопасностью легко управлять, а угрозы преувеличены. Они также выразили недовольство нехваткой средств для ведения дел и невозможностью нанять соответствующих специалистов по безопасности.

Около 59% признали, что отсутствие у их компаний навыков кибербезопасности было проблемой, а 62% изо всех сил пытались набрать необходимые навыки. Кроме того, 59% заявили, что их бюджет на кибербезопасность недостаточен. Еще 67% заявили, что сталкиваются с трудностями, чтобы быть в курсе событий в области кибербезопасности.

Инженер по глобальным решениям Sophos Аарон Бугал сказал, что необходимо устранить «тревожное отношение» к тому, что инциденты, связанные с кибербезопасностью, преувеличены…». ***(Eileen Yu. APAC firms face growing***

cyberattacks, take more than a week to remediate // ZDNet (https://www.zdnet.com/article/apac-firms-face-growing-cyberattacks-take-more-than-a-week-to-remediate/). 30.03.2021).

***

«Бразилия является мировым лидером в области фишинговых атак: согласно исследованиям, каждый пятый интернет-пользователь в стране подвергался атаке хотя бы один раз в 2020 году.

Согласно отчету о фишинге, подготовленном фирмой Kaspersky, занимающейся кибербезопасностью, Бразилия возглавляет список из пяти стран с самым высоким уровнем пользователей, подвергшихся краже данных за последний год. Другие упомянутые страны - Португалия, Франция, Тунис и Французская Гвиана.

Согласно исследованию, количество фишинговых атак на мобильные устройства только в период с февраля по март 2020 года увеличилось более чем на 120%. Факторы, лежащие в основе увеличения мошенничества, включают рост использования Интернета и доступа к онлайн-сервисам, таким как интернет-банкинг и мобильный банкинг, и онлайн-покупки в результате мер социального дистанцирования, а также широкомасштабное внедрение удаленной работы и беспокойство по поводу информации о пандемии.

Согласно исследованию, пандемия была постоянной темой фишинговых атак в течение 2020 года. Методы, используемые для получения учетных данных онлайн и банковских паролей, варьировались от веб-сайтов, предлагающих маски для лица и дезинфицирующие средства для рук в периоды дефицита, до поддельных веб-сайтов для регистрации в программах социальной помощи и, в последнее время, поддельных веб-страниц регистрации вакцины Covid-19.

С другой стороны, исследование «Лаборатории Касперского» отметило повышение уровня осведомленности пользователей Интернета об угрозах безопасности в Интернете. По этому поводу компания отметила, что, несмотря на рост фишинговых атак, был один конкретный аспект, который снизился по сравнению с 2019 годом: в том году более 30% бразильцев пытались хотя бы один раз открыть ссылка, которая привела на фишинговую страницу, по сравнению с примерно 20% в 2020 году.

«Это демонстрирует, что кампании и предупреждения об этом типе мошенничества означают, что пользователи более бдительны, но это не означает, что нам не нужно развиваться, поскольку статистика по-прежнему очень плохая», - сказал Фабио Ассолини, старший аналитик по безопасности в Kaspersky. Бразилия.

Более того, исследование отметило, что процент жертв фишинговых атак в Бразилии выше среднего мирового показателя - 20% против среднемирового показателя в 13%. По словам Ассолини, это несоответствие можно объяснить трудностями, с которыми пользователи Интернета в Бразилии сталкиваются при распознавании поддельных электронных писем: 30% бразильцев не могут определить, является ли электронное письмо подлинным, согласно предыдущему исследованию, проведенному фирмой по кибербезопасности.

«Нам необходимо улучшить наше цифровое образование», - отметил Ассолини. «[Неспособность распознавать угрозы] делает нас уязвимыми и склонными к участию в «обязательных рекламных акциях» и других онлайн-мошенничествах». ***(Angelica Mari. Brazil leads in phishing attacks // ZDNet (https://www.zdnet.com/article/brazil-leads-in-phishing-attacks/). 24.03.2021).***

***

«Служба Австралии сообщила Senate Estimates, что она сообщила в Австралийский центр кибербезопасности (ACSC) в 2019-2020 годах в общей сложности о 20 инцидентах в области кибербезопасности, которые охватывают его обязанности в Департаменте социальных услуг, Национальном агентстве по страхованию инвалидности и Департаменте ветеранов, помимо собственного IT-магазина.

ACSC сообщил о получении в общей сложности 436 уведомлений от государственных органов.

Генеральный директор Services Australia Ребекка Скиннер сказала, что, хотя было бы неуместно обсуждать природу инцидентов, ее агентство не имело нарушений данных граждан Австралии.

Как одна из крупнейших государственных организаций, Services Australia имеет свой собственный центр безопасности (SOC), который с 2017 года отвечает за защиту всех своих систем, в том числе тех, которые содержат информацию Centrelink, Medicare и алименты.

«Мы всегда проводим обзоры безопасности, обновления, исправления - такого рода вещи, чтобы поддерживать наши обязательства по отношению к основным восьми мерам безопасности ASD», - добавила она.

Скиннер сказал, что отдел кибербезопасности агентства блокирует около 14 миллионов подозрительных писем в месяц.

«Если что-то выглядит странно, люди что-то делают», - сказала она, отметив, что подразделение также обнаруживает несколько кампаний, пытающихся атаковать его системы. «Мы отслеживаем все это».

Главный информационный директор Services Australia Майкл Макнамара сказал, что SOC также «проводит собственное тестирование с точки зрения темной сети».

«У нас есть собственные внутренние возможности… которые постоянно работают над этим и выявляют проблемы в этой области», - сказал он сенаторам. «Мы не можем обсуждать какие-либо отдельные случаи, но мы очень, очень тесно работаем с AFP, ACSC и ASD».

Макнамара сказал, что, хотя многие его данные не классифицируются по классификации национальной безопасности, все они обрабатываются так же, как самые конфиденциальные и важные наборы данных агентства.

«Они проживают, если хотите, в центрах физической безопасности, которые эквивалентны видам, в которых вы бы защищали информацию о национальной безопасности, это просто технически, у них нет классификации национальной безопасности», - пояснил он.

«У нас есть очень надежная структура безопасности данных внутри агентства ... [включая] структуру целостности данных, которая рассматривает обучение нашего персонала использованию данных, о ненадлежащем и надлежащем использовании данных, распространении данных. Мы делаем это на постоянная основа."

Он сказал, что существует также ряд средств контроля доступа, таких как инструменты мониторинга, в дополнение к многофакторной аутентификации в агентстве и системах, которые оно контролирует.

«Наши системы, как вы понимаете, безопасны по самой своей природе и конструкции, а данные при хранении зашифрованы», - добавил он. «По мере того, как эти данные перемещаются, мы будем использовать наши инструменты мониторинга, чтобы контролировать перемещение, распространение этих данных, особенно если они покидают агентство».

По его словам, такие же требования предъявляются к ее крупнейшим подрядчикам - Telstra, Microsoft и IBM». ***(Asha Barbaschow. Services Australia reported 20 security incidents to the ACSC in 2019-20 // ZDNet (https://www.zdnet.com/article/services-australia-reported-20-security-incidents-to-the-acsc-in-2019-20/). 26.03.2021).***

***

«Кибератака нарушила прямые трансляции австралийского телеканала Channel Nine TV, что вызвало обеспокоенность по поводу уязвимости страны для хакеров.

Телекомпания заявила, что не может транслировать несколько шоу в воскресенье, в том числе Weekend Today.

Девять заявили, что расследуют, был ли взлом «преступным саботажем или работой иностранного государства».

Парламент Австралии также расследовал возможную кибератаку в Канберре в воскресенье.

Помощник министра обороны Эндрю Хасти сказал, что доступ к информационным технологиям и электронной почте в здании парламента был ограничен в качестве меры предосторожности. Он сказал, что это было сделано в ответ на проблемы, затрагивающие «внешнего поставщика», не вдаваясь в подробности.

«Это своевременное напоминание о том, что австралийцы не могут успокаиваться на своей кибербезопасности», - сказал министр сайту News.com.au в воскресенье.

«Правительство действовало быстро, и лучшие умы в мире работают над тем, чтобы Австралия оставалась самым безопасным местом для работы в Интернете», - сказал он.

Неясно, были ли связаны отключение работы парламента и кибератака на Девятом канале. Ведущие телеканала написали в Твиттере о своих проблемах в эфире.

Правительство Австралии, учреждения и крупные корпорации в последние годы стали жертвами серии кибератак.

В прошлом году премьер-министр Скотт Моррисон также предупредил, что австралийские организации становятся мишенью изощренных иностранных "государственных" хакеров.

Парламент Австралии и политические партии также пострадали от кибератаки в 2019 году.

Эксперты в области киберразведки говорят, что только несколько государств - Китай, Россия, Иран и Северная Корея - обладают потенциалом для таких атак и не являются союзниками Австралии.

Девять телеведущих Карл Стефанович пошутил о «русских» в телеканале Today Show в понедельник.

Эксперты давно связывают различные взломы в Австралии с Китаем, в том числе атаку на парламент в 2019 году.

Отношения между двумя странами за последние годы сильно ухудшились.

Что Девятый канал сказал о кибератаке?

Nine, которой также принадлежат газеты Sydney Morning Herald и The Age, заявила, что ее издательское и радиовещательное подразделения практически не пострадали.

Но его ТВ-раздел был. Сначала Nine заявила, что «решает технические проблемы», влияющие на прямую трансляцию.

Weekend Today, который работает с 07:00 до 13:00 по местному времени (с 21:00 до 03:00 по Гринвичу) из Сиднея, не транслировался.

Его новостной сайт в Интернете 9news.com.au также был затронут.

В воскресенье вечером Nine подтвердил, что на наши системы произошла «кибератака».

«Наши ИТ-команды работают круглосуточно, чтобы полностью восстановить наши системы, которые в первую очередь повлияли на наши вещательные и корпоративные бизнес-подразделения. Издательские и радиосистемы продолжают работать», - говорится в заявлении компании.

В более позднем отчете Марка Берроуза, старшего журналиста сети, говорится, что компания «подверглась атаке хакеров». Он сказал, что электронная почта и системы редактирования вышли из строя.

«Я не удивлен, - сказал Nine помощник министра обороны Хасти. «Только в прошлом году мы получили 60 000 сообщений о киберпреступлениях в кибербезопасность Австралии. Это сообщение каждые 10 минут».

Девять приказали всем своим сотрудникам работать дома до дальнейшего уведомления. Он смог показать свои шоу в понедельник». ***(Channel Nine cyber-attack disrupts live broadcasts in Australia // BBC (https://www.bbc.com/news/world-australia-56554641). 29.03.2021).***

***

«Злоумышленник насмехался над сайтом об открытых уязвимостях системы безопасности, что потребовало проверки кода.

MangaDex, онлайн-хранилище анимационных комиксов в стиле манга, будет закрыто до дальнейшего уведомления после инцидента со взломом.

На прошлой неделе сайт сообщил, что киберпреступник получил доступ к административной учетной записи «путем повторного использования токена сеанса, обнаруженного в старой утечке базы данных из-за неправильной конфигурации управления сеансом».

После устранения проблемы путем очистки всех сеансов глобально разработчики сайта посмотрели на код, который запускает MangaDex, пытаясь исправить любые уязвимости, с которыми они сталкивались в процессе работы. Однако, пока продолжалась проверка кода, тот же злоумышленник смог получить доступ к одной из учетных записей разработчиков MangaDex, похитив исходный код третьей версии сайта. Согласно MangaDex, вероятной мотивацией злоумышленника было «максимальное нарушение работы» сайта.

«Несмотря на то, что злоумышленник получил доступ к информации, которая обычно не видна из контекста обычного пользователя, мы не смогли подтвердить взлом полного хоста или взлом базы данных», - объявил сайт. «Как пользователь, мы будем поощрять вас предполагать, что ваши данные были взломаны, и немедленно принять меры предосторожности, такие как изменение паролей любых учетных записей, которые могут использовать тот же пароль, что и ваша учетная запись MangaDex. Настоятельно рекомендуется использовать менеджеры паролей для обеспечения безопасности вашей личности в Интернете».

Множественные уязвимости сайтов

Злоумышленник также издевался над операторами сайта, зная об ошибках безопасности в кодовой базе, что является основной причиной отключения MangaDex.

«Злоумышленник обновил репозиторий git, содержащий утечку исходного кода, заявив, что мы успешно исправили две из трех возможных CVE», - говорится в объявлении на веб-сайте, опубликованном в воскресенье. «Не имея возможности подтвердить заявления, мы предположили наихудший сценарий и закрыли сайт для дальнейшего расследования».

Управляемая волонтерами MangaDex планирует выделить необходимое время для завершения переписывания сайта, основанного на пятой версии исходного кода. По его оценке, это может занять до трех недель.

MangaDex планирует ускорить свое возвращение, выйдя в сеть после того, как будут готовы основные функции пятой версии: а именно, чтобы позволить читателям читать и следить за названиями манги, а также разрешить группам загружать «сканы» комиксов.

«Вместо того, чтобы поддерживать потенциально уязвимый веб-сайт и тратить наше время и усилия, играя в кошки-мышки с постоянными атаками от DDoS [распределенного отказа в обслуживании] до взлома, мы решили воспользоваться этой возможностью, чтобы переориентировать и ускорить нашу запланированную переработку сайт», согласно уведомлению. «Однако, вопреки нашим первоначальным планам, мы запустим эту версию 5, как только будут готовы минимальные необходимые функции».

Тем временем сайт пригласил этичных хакеров, чтобы они помогли найти уязвимости системы безопасности, заявленные злоумышленником в кодовой базе, а также любые другие недостатки.

Возможная программа Bug-Bounty

В то время как MangaDex в настоящее время полагается на добровольцев для поиска и исправления уязвимостей в системе безопасности (сайт сообщил, что эти помощники уже выявили «большое количество» ошибок, в ближайшее время может появиться более формальная программа.

«Мы по-прежнему открыты для любых предложений или ответственного раскрытия уязвимостей, обнаруженных в утечке исходного кода версии 3», - говорится в уведомлении. «Несмотря на то, что на момент написания мы обнаружили их множество и перешли к исправлению большинства из них, мы ценим все попытки помочь нам найти больше».

Кроме того, он сказал, что, как только новый сайт будет запущен, он может назначить награды за находки.

«Мы искренне намерены улучшить безопасность существующей и будущей инфраструктуры, и, хотя некоторые из наших разработчиков имеют опыт работы в области безопасности, мы решили, что наличие какой-либо формы программы bug-bounty для версии 5 только окажется целесообразным. выгодно для MangaDex», - говорится в уведомлении. «В качестве подтверждения этого мы намерены рассматривать выплаты в зависимости от серьезности обнаруженных ошибок. Более подробная информация будет опубликована в ближайшем будущем». ***(Tara Seals. MangaDex Site Offline Following Hacking Incident // Threatpost (https://threatpost.com/mangadex-site-offline-hacking/164983/). 23.03.2021).***

***

«Гигант социальных сетей уничтожил легионы поддельных профилей, нацеленных на распространение шпионского вредоносного ПО.

Facebook напал на группу хакеров в Китае, которые нацелены на уйгурскую этническую группу с помощью кибершпионажа.

Хакерская группа, известная как Earth Empusa или Evil Eye, нацелена на активистов, диссидентов и журналистов, причастных к уйгурскому сообществу, в первую очередь на тех, кто живет за границей в Австралии, Канаде, Казахстане, Сирии, Турции и США, среди других стран, используя поддельные аккаунты Facebook для фиктивных людей, симпатизирующих уйгурскому сообществу. Facebook заявил в среду, что группа рассылала вредоносные ссылки в сообщениях Facebook, которые при нажатии приводили к заражению вредоносными программами, ориентированными на шпионаж.

По данным Facebook, вредоносные ссылки вели к похожим доменам популярных уйгурских и турецких новостных сайтов, а также к взломанным легитимным веб-сайтам.

«Некоторые из этих веб-страниц содержали вредоносный код JavaScript, который напоминал ранее описанные эксплойты, которые устанавливали вредоносное ПО для iOS, известное как Insomnia, на устройства людей после их взлома», - сказал Майк Двилянски, глава отдела расследований кибершпионажа, и Натаниэль Глейхер, руководитель политики безопасности. написать в совместном посте в Facebook.

Согласно сообщению, все это было предпринято с помощью выборочного таргетинга: «Эта группа предприняла шаги для сокрытия своей активности и защиты вредоносных инструментов, заражая людей вредоносным ПО для iOS только после того, как они прошли определенные технические проверки, включая IP-адрес, операционную систему, браузер и страна и язык. "

Атаки вредоносного ПО для Android

Facebook удалил поддельные профили, но также обнаружил веб-сайты, созданные группой, имитирующие сторонние магазины приложений для Android, где они публиковали приложения на уйгурскую тематику. Согласно сообщению, они включали приложение для клавиатуры, приложение для молитв и приложение для словарей, которые были троянизированы с помощью двух вредоносных программ для Android - ActionSpy или PluginPhantom.

В Уйгуры, тюркский меньшинство этнической группы связаны с Центральной и Восточной Азии, которые ранее были направлены в других мобильных атак шпионских программ, в том числе кампании ActionSpy видели недавно, в июне.

Анализ последних вредоносных программ для Android показал, что, по данным Facebook, разработчиками некоторых инструментов, развернутых Earth Empusa, являются Beijing Best United Technology Co. и Dalian 9Rush Technology Co.

«Эти китайские фирмы, вероятно, являются частью разросшейся сети поставщиков с разной степенью операционной безопасности», - написали они, добавив, что FireEye предоставляет аналитические данные об угрозах, которые послужили основой для оценки Facebook.

«FireEye раскрыла операцию, нацеленную на уйгурское сообщество и других носителей китайского языка, с помощью вредоносных мобильных приложений, которые были разработаны для сбора обширной личной информации от жертв, включая местоположение GPS, SMS, списки контактов, снимки экрана, звук и нажатия клавиш», - сказал Бен Рид, директор по анализу. в Mandiant Threat Intelligence по электронной почте. «Эта операция активна как минимум с 2019 года и предназначена для длительного хранения на телефонах жертв, что позволяет операторам собирать огромные объемы личных данных».

Он добавил, что FireEye считает, что это мероприятие спонсируется государством. «В нескольких случаях китайские кибершпионажи использовали мобильное вредоносное ПО для нацеливания на уйгуров, тибетцев, гонконгских активистов демократии и других лиц, которые считались угрозой стабильности режима», - сказал он». ***(Tara Seals. Facebook Disrupts Spy Effort Aimed at Uyghurs // Threatpost (https://threatpost.com/facebook-disrupts-spy-uyghurs/165032/). 25.03.2021).***

***

«QNAP предупреждает клиентов о продолжающихся атаках на устройства QNAP NAS (сетевые хранилища) и призывает их как можно скорее усилить свою безопасность.

В этих атаках злоумышленники используют автоматизированные инструменты для входа в открытые для доступа в Интернет устройства NAS,

используя пароли, созданные на месте или из списков ранее скомпрометированных учетных данных.

«Недавно QNAP получил несколько отчетов пользователей о попытках хакеров войти в систему на устройствах QNAP, используя атаки методом грубой силы, при которых хакеры испробовали все возможные комбинации паролей для учетной записи пользователя устройства QNAP», - предупредила компания.

«Если используется простой, ненадежный или предсказуемый пароль (например, «пароль» или «12345»), хакеры могут легко получить доступ к устройству, нарушив безопасность, конфиденциальность и конфиденциальность».

После подбора правильной комбинации они получают полный доступ к целевому устройству, позволяя им получить доступ и украсть конфиденциальные документы или развернуть вредоносное ПО.

Если злоумышленникам не удается проникнуть в систему методом перебора, системные журналы устройств NAS будут записывать попытки и записывать их с предупреждающими сообщениями «Не удалось войти в систему»…». ***(Sergiu Gatlan. QNAP warns of ongoing brute-force attacks against NAS devices // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/qnap-warns-of-ongoing-brute-force-attacks-against-nas-devices/). 25.03.2021).***

***

«Специалисты Positive Technologies, проанализировав киберугрозы последнего квартала 2020 г., выявили по всему миру рост числа атак, направленных на торговые компании и медучреждения. Еще одной тенденцией стало увеличение числа атак на частных лиц с использованием методов социальной инженерии.

В течение всего 2020 г. эксперты наблюдали ежеквартальное увеличение числа киберинцидентов и IV квартал не стал исключением. Количество атак по сравнению с III кварталом выросло на 3,1%, а в сравнении с аналогичным периодом 2019 г. рост составил 42,2%. Ранее отмеченный тренд на переход от социальной инженерии к методам хакинга в атаках на организации укрепился и в IV квартале. В инцидентах с частными лицами, напротив, эксперты зафиксировали всплеск применения техник социальной инженерии, доля этого метода выросла с 67% в III квартале до 86%.

Исследование показывает, что количество атак на отрасль торговли увеличилось на 56% в сравнении с III кварталом и достигло абсолютного максимума за последние два года. Около трети атак в этой сфере были проведены операторами программ-вымогателей, как, например, в случае с атакой на южнокорейского ретейлера E-Land. В каждой пятой атаке на торговые предприятия использовались веб-скиммеры, которые злоумышленники размещали на взломанных сайтах магазинов.

«Чаще всего в ходе атак на торговлю злоумышленники похищают данные платежных карт, к примеру в IV квартале их доля среди всей украденной информации составила 33%, — сказала аналитик Positive Technologies Яна Юракова. — На втором месте по популярности персональные данные клиентов (27%) и на третьем — учетные данные (20%)».

Под шквал атак также попали фармацевтические компании, участвующие в цепочке производства и поставки вакцины от COVID-19, например Fareva, Dr. Reddy's и Johnson & Johnson. Злоумышленники не только пытаются украсть наработки и сорвать производство, но и продолжают эксплуатировать интерес обычных людей к теме вакцины. По данным исследования, в IV квартале около 40% всех фишинговых рассылок на тему пандемии были посвящены вакцине.

В последнем квартале 2020 г. аналитики Positive Technologies вновь отметили рост числа атак с использованием шифровальщиков, их доля составила 56% среди всех атак с использованием вредоносного ПО. Больше всего атак замечено в отношении медицинских (20%) и государственных учреждений (19%), а также промышленных компаний (11%). Среди наиболее активных программ-шифровальщиков — Ryuk, REvil, Clop, Egregor и DoppelPaymer.

Для защиты от кибератак специалисты Positive Technologies советуют, прежде всего, придерживаться общих рекомендаций по обеспечению корпоративной и личной кибербезопасности. Для простоты выявления и устранения недостатков инфраструктуры эксперты рекомендуют выстроить автоматизированный процесс управления уязвимостями. Помимо этого, следует использовать современные средства защиты, включая межсетевые экраны уровня веб-приложений, средства анализа сетевого трафика, SIEM-системы. Для предотвращения атак, связанных с доставкой вредоносных программ по электронной почте, необходимо проверять вложения в песочнице — специальной виртуальной среде, предназначенной для анализа поведения файлов». ***(Эксперты Positive Technologies зафиксировали резкий рост числа атак на торговые предприятия // CNews (https://safe.cnews.ru/news/line/2021-03-29_eksperty_positive_technologies_zafiksirovali). 29.03.2021).***

***

«Производитель оборудования для аэрокосмической и энергетической промышленности Honeywell сообщил об атаке вредоносного ПО на свои сети. Как пояснили в компании, вредонос вывел из строя "ограниченное количество" ее компьютерных систем, и к настоящему времени сервисы Honeywell снова заработали. Характер кибератаки, в том числе использовалось ли в ней вымогательское ПО, компания не сообщает.

"В настоящее время мы не ожидаем, что этот инцидент окажет существенное влияние на Honeywell. Мы оперативно приняли меры по устранению инцидента, в том числе установили партнерские отношения с Microsoft для оценки и исправления ситуации. С тех пор наши системы были защищены, мы выявили точку входа, и несанкционированный доступ был полностью заблокирован. Мы также уведомили правоохранительные органы", - сообщила компания.

Расследование продолжается, но на данный момент специалисты пока не обнаружили никаких свидетельств того, что злоумышленники похитили данные клиентов.

"Если мы обнаружим, что какая-либо информация о клиентах была украдена, мы свяжемся с этими клиентами напрямую", - пообещали в Honeywell».

(Промышленный гигант Honeywell восстановился после кибератаки // SecurityLab.ru (https://www.securitylab.ru/news/517728.php). 24.03.2021)

***

«В 2020 году центр мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком-Солар» выявил и отразил свыше 1,9 млн атак, что на 73% превышает прошлогодний показатель. При этом эксперты впервые выделяют как тренд рост числа атак типа supply chain (проникновение через инфраструктуру подрядчика): за год количество подобных инцидентов в отношении объектов критической инфраструктуры увеличилось в два раза. Это следует из подготовленного компанией ежегодного отчета Solar JSOC Security Report.

Взлом подрядчика стал самым эффективным методом для проникновения в целевые для киберпреступников инфраструктуры, среди которых, как правило, крупнейшие федеральные организации госсектора и объекты КИИ. Это подтверждается и международным опытом. В конце 2020 года стало известно о взломе компании-разработчика ПО SolarWinds, вследствие чего пострадали такие ее клиенты, как Microsoft, Cisco, FireEye, а также несколько ключевых министерств и ведомств США. Аналогичные попытки атак на органы власти и объекты КИИ Solar JSOC фиксирует и в России.

Активное использование метода supply chain связано с ростом числа более сложных целенаправленных атак. Кроме того, все чаще организации отдают на аутсорсинг часть внутренних процессов, но при этом редко мониторят собственную инфраструктуру и практически не контролируют точки подключения сторонних компаний к своей сети. В итоге проблема может долгое время оставаться вне фокуса внимания. Именно это привело к росту подобных атак в последний год.

«Рост популярности метода supply chain указывает не просто на изменение технической специфики атак, а на появление новой ключевой угрозы кибербезопасности на государственном уровне. Однако четкого решения, как минимизировать риски, пока нет. Даже аттестованный регулятором на соответствие нормам ИБ подрядчик может быть успешно атакован злоумышленниками. При этом у компании-заказчика нет возможности напрямую контролировать уровень ИБ-защиты аутсорсера. Очевидно, что продвинутые APT-группировки будут все чаще использовать технику supply chain, поэтому ИБ-сообществу нужно как можно скорее выработать фундаментальный подход к решению проблемы», - отметил Владимир Дрюков, директор центра мониторинга и реагирования на кибератаки Solar JSOC компании «Ростелеком-Солар».

Также впервые с 2017 года эксперты Solar JSOC фиксируют рост нарушений, совершаемых внутренними пользователями – рядовыми сотрудниками компаний. Больше половины (53%) внутренних инцидентов были связаны с утечками информации: перейдя на удаленный режим работы, сотрудники стали совершать нарушения, включая хищение и слив данных, на которые не решились бы в офисе. Кроме того, пандемия привела к росту нарушений в части доступа в интернет. Речь идет не только о посещении подозрительных сайтов с рабочего компьютера.

Удаленные работники могли также получить нелегитимный доступ к закрытым ресурсам компании, так как корректно сегментировать корпоративную сеть на базе VPN затруднительно.

Самым распространенным инструментом внешних злоумышленников стало вредоносное ПО, а основным способом его доставки в инфраструктуру жертвы - фишинговые рассылки, большая часть которых спекулировала на теме COVID-19. При этом отмечается значительный рост (на треть) числа атак с использованием шифровальщиков: в период массовой «удаленки», когда многие компании ослабили ИБ-защиту, этот и без того простой способ монетизации стал еще популярнее.

В 2020 году на 30% выросло количество атак, направленных на получение контроля над инфраструктурой, в то время как количество атак, нацеленных на кражу денежных средств, увеличилось незначительно (менее, чем на 10%). Это говорит о значительном росте квалификации злоумышленников и усложнении их инструментария». ***(Зафиксирован двукратный рост атак на КИИ через инфраструктуры подрядчиков // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5726019-Zafiksirovan-dvukratnyj-rost-atak.html). 26.03.2021).***

***

Діяльність хакерів та хакерські угруповування

«Кампания кибершпионажа нацелена на телекоммуникационные компании по всему миру с помощью атак с использованием вредоносных загрузок с целью кражи конфиденциальных данных, в том числе информации о технологии 5G, от скомпрометированных жертв.

…кампания ориентирована на телекоммуникационных провайдеров в Юго - Восточной Азии, Европе и Соединенных Штатах. Исследователи говорят, что атаки, получившие название Operation Diànxùn, являются делом работы хакерской группы, известной как Mustang Panda и RedDelta, работающей из Китая…

Предполагается, что по меньшей мере 23 провайдера телекоммуникационных услуг стали жертвами кампании, которая началась по крайней мере с августа 2020 года. Не разглашается, сколько целей было успешно взломано хакерами.

Хотя первоначальные средства заражения еще не определены, известно, что жертвы направлены на вредоносный фишинговый домен, находящийся под контролем злоумышленников, который используется для доставки вредоносного ПО жертвам.

По словам исследователей, вредоносная веб-страница маскируется под сайт вакансий Huawei, который был разработан так, чтобы выглядеть неотличимо от настоящего. Исследователи подчеркнули, что сама Huawei не участвует в кибершпионажной кампании.

Когда пользователи посещают фальшивый сайт, он доставляет вредоносное Flash-приложение, которое используется для установки бэкдора Cobalt Strike на посещающую машину, что в конечном итоге обеспечивает злоумышленникам

видимость машины и возможность собирать и красть конфиденциальную информацию…

Исследователи связали операцию Diànxùn с предыдущими хакерскими операциями китайских групп из-за атак и развертывания вредоносного ПО с использованием аналогичных тактик, методов и процедур (ДТС), которые использовались в предыдущих кампаниях, публично приписываемых группе…

«Мы считаем, что кампания все еще продолжается. На прошлой неделе мы заметили новую активность с теми же ДТС, что означает, что действующий субъект и кампания все еще работают», - сказал ZDNet Томас Рочча, исследователь безопасности в группе стратегической разведки McAfee.

Поскольку вредоносные домены играют такую важную роль в этой кампании, одним из способов защиты от атак может быть обучение персонала умению распознавать, были ли они направлены на поддельный или вредоносный веб-сайт - хотя с учетом того, что кибер-злоумышленники стали очень хорошо умеет создавать высокоточные поддельные сайты, это может быть непросто…». ***(Danny Palmer. Hackers are targeting telecom companies to steal 5G secrets // ZDNet (https://www.zdnet.com/article/hackers-are-targeting-telecoms-companies-to-steal-5g-secrets/). 16.03.2021).***

***

«В 2020 году хакеры заработали рекордные 40 миллионов долларов (28 миллионов фунтов стерлингов) за сообщения о недостатках программного обеспечения через ведущую службу отчетов об ошибках.

HackerOne сообщила, что девять хакеров заработали более 1 миллиона долларов каждый после того, как сообщила о своих результатах пострадавшим организациям.

Один румын, который начал заниматься поиском ошибок всего два года назад, увидел, что на сегодняшний день его общий доход превышает 2 миллиона долларов. Самый высокооплачиваемый хакер Великобритании в прошлом году заработал 370 000 долларов.

Платформа предположила, что пандемия дала волонтерам больше времени для продолжения работы.

Исследование, проведенное HackerOne, показало, что 38% участников потратили больше времени на взлом с момента начала вспышки Covid-19.

'Буквально трясется'

Многие из них работают неполный рабочий день и базируются в десятках разных стран, включая США, Аргентину, Китай, Индию, Нигерию и Египет.

Присужденная сумма денег зависит от серьезности недостатка и может варьироваться от менее 140 долларов до гораздо более крупных сумм.

Компания HackerOne, базирующаяся в Калифорнии, взимает с предприятий абонентскую плату за использование своей платформы.

Британская охотница за «багами» Кэти Пакстон-Страх, преподаватель Манчестерского столичного университета, говорит, что в свободное время ищет ошибки.

Хотя деньги хорошие, она говорит, что это не способ быстро разбогатеть.

«Я помню, как обнаружила свою первую ошибку, буквально встряхнулась и поняла: «Вау, я только что спасла людей от довольно большой ошибки».

«Я не просто использую свое время, чтобы выиграть приз, я активно помогаю защищать приложения, которые использую, поэтому для меня это вызов, смешанный с занятием чем-то хорошим».

Другая аналогичная платформа под названием YesWeHack, базирующаяся во Франции, заявила, что ее 22000 хакеров нашли вдвое больше ошибок в 2020 году, чем в предыдущем году.

Он не публикует данные о денежных вознаграждениях, полученных через его сервис.

«Принимая во внимание новые риски и важность кибербезопасности для экономического выживания компаний, все большее число руководителей информационной безопасности обращаются за помощью в поисках ошибок», - сказал генеральный директор Гийом Вассо-Ульер (Guillaume Vassault-Houlière).

Другой сервис, BugCrowd, заявил, что за последние 12 месяцев количество заявок на его платформе увеличилось на 50%.

Скептик щедрости

Популярность коммерческих программ поиска ошибок возросла за последние пять лет, но некоторые эксперты считают, что в системе есть недостатки, если на них слишком сильно полагаться.

Исследователь безопасности Виктор Геверс, который руководит фондом GDI Foundation по ответственному раскрытию информации в Нидерландах, сказал, что никогда не брал денег за обнаруженные им ошибки.

«Но для начинающих исследователей в области безопасности или студентов эти коммерческие платформы для вознаграждений за обнаруженные ошибки великолепны, поскольку они предлагают много средств защиты, ресурсов и являются идеальным местом для начала». ***(Joe Tidy. Covid: White hat bounty hackers become millionaires // BBC (https://www.bbc.com/news/technology-56350362). 10.03.2021).***

***

«Хакеры получили доступ к камерам видеонаблюдения, установленным в Tesla, Equinox, медицинских клиниках, тюрьмах и банках, включая Bank of Utah.

В дополнение к изображениям, снятым с камер, хакер также поделился скриншотами своей способности получить доступ к корневой оболочке систем наблюдения, используемых Cloudflare и в штаб-квартире Telsa.

Взламывает несколько камер в #OperationPanopticon

По словам Тилли Коттманн, реверс-инженера группы хакеров, они получили доступ к этим системам наблюдения, используя учетную запись суперадминистратора Verkada, компании наблюдения, которая работает со всеми этими организациями.

…Коттманн сказал, что они нашли жестко запрограммированные учетные данные для учетной записи суперадминистратора Verkada в открытой инфраструктуре DevOps.

Verkada производит корпоративные системы безопасности, такие как автоматизация и камеры наблюдения IoT. Также известно, что компания предоставляет услуги Tesla.

Сегодня днем Коттманн подразнил, опубликовав несколько изображений, якобы снятых с камер наблюдения в Equinox, Tesla и Bank of Utah.

В той же ветке Twitter Коттманн поделился изображениями того, что выглядело как root-доступ к операционной системе Linux. На этих изображениях вы можете увидеть MAC-адрес одной из сетевых карт, который соответствует оборудованию, разработанному компанией Verkada.

После того как Bloomberg News, первым сообщивший об этой атаке, связался с Веркадой, хакеры потеряли доступ к взломанной учетной записи суперадминистратора.

«Мы отключили все учетные записи внутренних администраторов, чтобы предотвратить любой несанкционированный доступ. Наша группа внутренней безопасности и внешняя служба безопасности исследуют масштаб и масштаб этой проблемы, и мы уведомили правоохранительные органы», - сказал Веркада…

Cloudflare сообщил BleepingComputer, что камеры были расположены в офисах, которые были закрыты в течение нескольких месяцев, и что нарушение не повлияло на их клиентов.

«Сегодня днем нас предупредили, что система видеонаблюдения Verkada, которая контролирует основные точки входа и основные проезды в нескольких офисах Cloudflare, могла быть взломана. Камеры были расположены в нескольких офисах, которые были официально закрыты в течение нескольких месяцев.

Как только нам стало известно о компрометации, мы отключили камеры и отключили их от офисных сетей. Для ясности: этот инцидент не повлиял на продукты Cloudflare, и у нас нет оснований полагать, что инцидент с офисными камерами видеонаблюдения повлияет на клиентов». - Cloudflare

Хэштег #OperationPanopticon, связанный с этой кибератакой, относится к Panopticon, философской концепции дизайна.

Паноптикум относится к конструкции такого здания, в которой пленники (например, заключенные) не могут сказать, наблюдают ли за ними сотрудники службы безопасности или нет в данный момент.

Это означает, что в здании с большим количеством заключенных один охранник может быть не в состоянии контролировать всех заключенных одновременно, но из-за идеологии дизайна паноптикумов каждый заключенный может бояться, что за ним наблюдают, потому что у них нет возможности знать, если они наблюдают…». ***(Ax Sharma. Hackers access surveillance cameras at Tesla, Cloudflare, banks, more // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-access-surveillance-cameras-at-tesla-cloudflare-banks-more/). 09.03.2021).***

***

«Кибергруппировка REvil объявила об успешной атаке на корпорацию Acer, одного из крупнейших в мире производителей электроники. С жертвы требуют около $50 млн.

18 марта 2021 г. члены REvil опубликовали на своем сайте несколько изображений, которые должны подтвердить аутентичность украденной информации, — шифровальщик REvil не только шифрует, но и выводит данные из атакованной им инфраструктуры.

По данным Bleeping Computer, злоумышленники вывесили финансовые таблицы, информацию о банковских счетах и соответствующую переписку. Со стороны Acer пока не поступало однозначных подтверждений или опровержений, но комментарии ее пресс-службы явственно указывают на то, что что-то все-таки происходит:

«Acer постоянно мониторит свои ИТ-системы, и большая часть оказываются успешно отражены, — говорится в заявлении пострадавшей стороны. — Такие компании как наша все время подвергаются нападениям, и мы сообщили о недавно обнаруженных аномальных ситуациях соответствующим правоохранительным органам и органам власти, занимающимся защитой данных, в нескольких странах».

Вечером 22 марта 2021 г. авторизованный аккаунт Acer в социальной сети Twitter отреагировал на сообщение пользователя из Германии о том, что сайт компании для обслуживания аппаратуры компании «лежит уже неделю» Представитель Acer подтвердил, что из-за временной недоступности сетей следует обратиться в службу поддержки по телефону.

Затребованная сумма выкупа в $50 млн, вероятно, поставит рекорд: до сих пор максимальным был выкуп, который злоумышленники потребовали от фирмы Grubman Shire Meiselas & Sacks в мае 2020 г. — $42 млн. В этот раз операторы REvil грозятся поднять выкуп вдвое, если деньги не переведут на их счета в течение восьми дней.

В материале издания Engadget высказывается предположение, что атака стала возможной благодаря относительно недавно обнаруженной уязвимости в Micosoft Exchange. Хотя патчи к ней доступны уже в течение некоторого времени, обновление уязвимых серверов происходит далеко не сразу.

«Если это так, то злоумышленники успешно воспользовались “окном возможностей”, возникшем вследствие нерасторопности ИТ-отделов Acer, — полагает Анастасия Мельникова, эксперт по информационной безопасности компании SEC Consult Services. — Но, опять же, в данной ситуации очень много “если”. Еще не факт, что у Acer что-то украли и что это стоит тех денег, которые от фирмы требуют шантажисты. Даже в худшем случае, впрочем, Acer не стоит платить ни цента. Каждая успешная такая операция убеждает злоумышленников в перспективности их деятельности, а заодно приводит к увеличению рядов желающих провернуть что-то подобное». ***(Хакеры зашифровали данные Acer // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5725436-Xakery-zashifrovali-dannye-Acer.html). 23.03.2021).***

***

«APT-группировку, связанную с китайским правительством, обвиняют в кибератаке на парламент Финляндии.

Финская Служба безопасности и разведки (Supo) сообщила, что за кибершпионской кампанией, целью которой был финский парламент, стоит APT31.

По словам Supo, она идентифицировала операцию по кибершпионажу, спонсируемую государством, целью которой было проникновение в IT-системы парламента. Служба считает, что атаку совершила APT31.

В результате атаки был взломан ряд парламентских учетных записей электронной почты.

Все еще выясняется цель атаки.

Также Supo сообщила, что с момента атаки парламент принял меры, чтобы усилить информационную безопасность». ***(Группировку APT31 обвинили в кибератаке на парламент Финляндии // SecureNews (https://securenews.ru/apt31-group-accused-of-cyberattack-on-finnish-parliament/). 22.03.2021).***

***

Вірусне та інше шкідливе програмне забезпечення

«Исследователи из Palo Alto Networks сообщают, что в течение последнего месяца был замечен вариант ботнета Mirai, нацеленный на новые уязвимости системы безопасности в течение нескольких часов после того, как они были публично раскрыты.

Примерно с 2016 года исходный код Mirai просочился в сеть, в результате чего выпущено десятки вариантов, каждый со своими возможностями таргетинга.

Вариант, отслеживаемый Palo Alto Networks, отличается тем, что в течение четырех недель он начал использовать несколько уязвимостей, которые были обнаружены в этом году.

23 февраля был замечен вариант Mirai, нацеленный на CVE-2021-27561 и CVE-2021-27562 - две уязвимости в платформе Yealink DM (Device Management), которые были обнаружены в тот же день.

Что касается Yealink DM версии 3.6.0.20 и старше, недостатки (SSRF до авторизации и внедрение команд соответственно) существуют, потому что предоставленные пользователем данные не фильтруются должным образом и могут быть использованы для выполнения произвольных команд от имени root-пользователя без аутентификации.

3 марта исследователи безопасности Palo Alto Networks заметили, что те же образцы также использовали эксплойт для CVE-2021-22502, критической уязвимости (оценка CVSS 9,8) удаленного выполнения кода в Micro Focus Operations Bridge Reporter.

Ошибка безопасности, доступная для использования без аутентификации, существует из-за того, что введенная пользователем строка не проверяется должным образом при обработке параметра Token, предоставленного конечной точке LogonResource, что позволяет злоумышленнику выполнить код от имени root-пользователя.

Десять дней спустя, 13 марта, образцы также включали эксплойт, нацеленный на CVE-2020-26919, критическую уязвимость (оценка CVSS 9,8), затрагивающую гигабитные коммутаторы бизнес-класса NETGEAR JGS516PE.

Ошибка описывается как «отсутствие контроля доступа на функциональном уровне»…

«На момент написания этой статьи атаки еще продолжаются. После успешной эксплуатации злоумышленники пытаются загрузить вредоносный сценарий оболочки, который содержит дополнительные способы заражения, такие как загрузка и выполнение вариантов Mirai и брутфорсеров», - сообщает Palo Alto Networks». ***(Ionut Arghire. New Mirai Variant Leverages 10 Vulnerabilities to Hijack IoT Devices // Wired Business Media (https://www.securityweek.com/new-mirai-variant-leverages-10-vulnerabilities-hijack-iot-devices). 17.03.2021).***

***

«Активная киберпреступная хакерская операция заключается в распространении нового вредоносного ПО, написанного на языке программирования, который редко используется для компиляции вредоносного кода…

Вредоносное ПО NimzaLoader предназначено для предоставления злоумышленникам доступа к компьютерам с Windows и возможности выполнять команды - то, что может дать тем, кто контролирует вредоносное ПО, возможность управлять машиной, красть конфиденциальную информацию или потенциально развертывать дополнительные вредоносные программы.

Предполагается, что вредоносная программа является результатом работы киберпреступной хакерской группы, которую Proofpoint называет TA800, хакерской операции, нацеленной на широкий спектр отраслей по всей Северной Америке.

Группа обычно связана с BazarLoader, разновидностью троянского вредоносного ПО, которое создает полный бэкдор на скомпрометированных машинах Windows и, как известно, используется для проведения атак программ-вымогателей.

Как и BazarLoader, NimzaLoader распространяется с использованием фишинговых писем, которые связывают потенциальных жертв с поддельным загрузчиком PDF, который при запуске загрузит вредоносное ПО на машину. По крайней мере, некоторые из фишинговых писем предназначены для конкретных целей с настраиваемыми ссылками, включающими личные данные, такие как имя получателя и компанию, в которой он работает.

Шаблон сообщений и способ, которым атака пытается доставить полезную нагрузку, соответствуют предыдущим фишинговым кампаниям TA800, что привело исследователей к выводу, что NimzaLoader также является продуктом того, что уже было плодотворной хакерской операцией, которая теперь добавила еще одно средство атака…

Поскольку фишинг является основным средством распространения NimzaLoader, поэтому рекомендуется, чтобы организации обеспечивали безопасность своей сети с помощью инструментов, которые в первую очередь помогают предотвратить попадание вредоносных писем во входящие…». ***(Danny Palmer. This malware was written in an unusual programming language to stop it***

from being detected // ZDNet (https://www.zdnet.com/article/this-malware-was-written-in-an-unusual-programming-language-to-stop-it-from-being-detected/). 11.03.2021).

***

«Новый вариант ботнета Gafgyt, который активно нацелен на уязвимые устройства D-Link и Интернета вещей, является первым вариантом вредоносного ПО, которое полагается на коммуникации Tor.

Исследователи обнаружили, что это первый вариант семейства ботнетов Gafgyt, скрывающий свою деятельность с помощью сети Tor.

Ботнет Gafgyt, обнаруженный в 2014 году, стал печально известен благодаря запуску крупномасштабных распределенных атак типа «отказ в обслуживании» (DDoS). Исследователи впервые обнаружили активность новейшего варианта, который они назвали Gafgyt_tor, 15 февраля.

Чтобы избежать обнаружения, Gafgyt_tor использует Tor для сокрытия своих командно-управляющих сообщений (C2) и шифрует конфиденциальные строки в образцах. В использовании Tor семейством вредоносных программ нет ничего нового; однако исследователи заявили, что до сих пор не видели, чтобы Гафгит использовал сеть анонимности.

Ботнет Gafgyt_tor: распространение и новые функции

Ботнет в основном распространяется через слабые пароли Telnet - распространенная проблема на устройствах Интернета вещей - и за счет использования трех уязвимостей. Эти уязвимости включают ошибку удаленного выполнения кода (CVE-2019-16920) в устройствах D-Link; уязвимость удаленного выполнения кода в программном обеспечении корпоративного портала Liferay (для которого нет CVE); и недостаток (CVE-2019-19781) в Citrix Application Delivery Controller.

«Исходная функция initConnection (), которая отвечает за установление соединения C2, исчезла, ее заменил большой участок кода, отвечающий за установление соединения Tor», - заявили исследователи.

Новые возможности Tor, команды

В этом большом разделе кода существует tor_socket_init, функция, которая отвечает за инициализацию списка прокси-узлов с IP-адресами и портом. Исследователи заявили, что таким образом можно встроить более 100 прокси Tor - и новые образцы постоянно обновляют список прокси.

«После инициализации списка прокси образец выберет случайный узел из списка, чтобы включить связь Tor через tor_retrieve_addr и tor_retrieve_port», - заявили исследователи.

После установления соединения с C2 ботнет запрашивает wvp3te7pkfczmnnl.onion через даркнет, от которого ожидает команд.

«Основной функцией Gafgyt_tor по-прежнему являются DDoS-атаки и сканирование, поэтому он в основном следует общей директиве Gafgyt», - сказали исследователи. В ботнет также была добавлена новая директива LDSERVER, которая позволяет C2 быстро указывать серверы, с которых загружаются полезные данные. По словам исследователей, это позволяет злоумышленникам быстро

переключаться между курсами, если сервер загрузки, принадлежащий злоумышленнику, будет обнаружен и заблокирован.

Ссылки на Freak Threat Actor, другие бот-сети

Исследователи заявили, что этот вариант имеет то же происхождение, что и образцы Gafgyt, распространяемые группой угроз, которую исследователи NetLab 360 называют группой keksec, а другие исследователи называют актором угрозы Freak. По их словам, группа keksec повторно использует код и IP-адреса между различными другими семействами ботов, включая ботнет Tsunami, а также семейство ботнетов Necro, обнаруженных в январе.

«Мы думаем, что Gafgyt_tor и Necro, скорее всего, управляются одной и той же группой людей, у которых есть пул IP-адресов и несколько исходных кодов ботнетов, а также возможность непрерывного развития», - заявили исследователи. «На практике они образуют разные семейства ботнетов, но повторно используют инфраструктуру, такую как IP-адрес».

Другие варианты ботнета Gafgyt

Gafgyt.tor - это всего лишь последний обнаруженный вариант популярного ботнета. В 2019 году исследователи предупредили о новом варианте Gafgyt, который добавляет уязвимые устройства IoT в свой арсенал ботнетов и использует их для выхода из строя игровых серверов по всему миру.

В 2018 году исследователи заявили, что они обнаружили новые варианты ботнетов Mirai и Gafgyt IoT, нацеленные на известные уязвимости в Apache Struts и SonicWall; а также отдельная атака с активным запуском двух ботнет- кампаний IoT / Linux с использованием ошибок CVE-2018-10562 и CVE-2018-10561 в маршрутизаторах Dasan.

Совсем недавно, в прошлом году, появился ботнет Hoaxcalls как вариант семейства Gafgyt. Ботнет, который можно использовать для крупномасштабных распределенных кампаний отказа в обслуживании (DDoS), распространяется через незащищенную уязвимость, влияющую на ZyXEL Cloud CNM SecuManager». ***(Lindsey O'Donnell. D-Link, IoT Devices Under Attack By Tor-Based Gafgyt Variant // Threatpost (https://threatpost.com/d-link-iot-tor-gafgyt-variant/164529/). 05.03.2021).***

***

«Никогда прежде не используемая программа-дроппер, Clast82, извлекает вредоносные программы AlienBot и MRAT в рамках продуманной кампании Google Play, нацеленной на пользователей Android.

…вредоносная программа-дроппер, позволяющая злоумышленникам удаленно красть данные с телефонов Android, распространяется через девять вредоносных приложений в официальном магазине Google Play.

По данным Check Point Research, вредоносная программа является частью кампании, направленной на сбор финансовой информации о жертвах, но которая также позволяет в конечном итоге захватить мобильные телефоны.

Дроппер, получивший название Clast82, был замаскирован под безобидные приложения, которые не извлекают вредоносную полезную нагрузку, пока они не будут проверены и очищены Google Play Protect. Google Play Protect - это механизм

оценки магазина, предназначенный для отсеивания приложений со злым умыслом и вредоносных функций.

«Во время ознакомительного периода Clast82 в Google Play конфигурация, отправленная с [Google] Firebase [командно-управляющий сервер], содержит параметр «enable», - говорится в исследовании Check Point. «В зависимости от значения параметра вредоносная программа решит, инициировать вредоносное поведение или нет. Для этого параметра установлено значение «false», а значение «true» изменится только после того, как Google опубликует вредоносное ПО Clast82 в Google Play».

После размещения в App Store Clast82 загружает банковского трояна AlienBot или, в некоторых случаях, MRAT, как установило расследование.

Инфо-крадеры AlienBot и MRAT

Check Point отметила, что AlienBot доступен в модели «вредоносное ПО как услуга» (MaaS) и позволяет удаленному злоумышленнику внедрять вредоносный код в законные финансовые приложения.

«Злоумышленник получает доступ к учетным записям жертв и в конечном итоге полностью контролирует их устройство», - говорится в анализе компании. «Получив контроль над устройством, злоумышленник имеет возможность управлять определенными функциями, как если бы они удерживали устройство физически, например, устанавливая новое приложение на устройство или даже управляя им с помощью TeamViewer».

Между тем MRAT существует по крайней мере с 2014 года, когда он использовался против протестующих в Гонконге. Он был создан для разведки и сбора информации и обладает всеми типичными функциями шпионского ПО, а также уклонением от обнаружения, специальным проверкам на наличие вирусов, функциями удаления приложений и файлов и т. д.

Обе полезные загрузки были размещены на GitHub. AlienBot был, безусловно, самым распространенным средством доставки жертвам.

«В случае Clast82 мы смогли идентифицировать более 100 уникальных полезных загрузок AlienBot, банкира Android MaaS, нацеленного на финансовые приложения и пытающегося украсть учетные данные и коды 2FA [двухфакторной аутентификации] для этих приложений», - отметили исследователи.

Проекты GitHub, связанные с вредоносными приложениями для Android

Анализ Check Point показал, что для каждого приложения субъект создавал нового пользователя-разработчика для магазина Google Play вместе с соответствующим репозиторием кода в GitHub.

Например, вредоносное приложение Cake VPN основано на законном репозитории GitHub.

Для всех поддельных учетных записей разработчиков в Google Play был указан один адрес электронной почты для контактной информации: sbarkas77590@gmail.com. Кроме того, в описании каждого приложения использовалась одна и та же страница политики, которая, в свою очередь, была связана с одним и тем же репозиторием GitHub. Очевидно, что все приложения были работой одного автора.

Поток заражения вредоносным ПО Clast82

Обычно одно действие в любом приложении Android указывается как «основное» действие (MainActivity.java), которое предоставляется пользователю при запуске приложения. В этом случае, когда пользователь запускает приложение Clast82, MainActivity запускает службу переднего плана для выполнения вредоносной задачи удаления, как обнаружила Check Point.

Этот сервис просто называется «LoaderService».

«Как только пользователь загружает одно из поддельных приложений и запускает его, он запускает службу из MainActivity, которая запускает поток сброса под названием LoaderService». «Служба переднего плана регистрирует слушателя для базы данных реального времени Firebase, из которой получает путь полезной нагрузки от GitHub».

Правила разработчика Android указывают, что когда приложение создает подобную службу переднего плана, оно должно постоянно показывать пользователю уведомление о том, что делает приложение.

«Clast82 обошел это, показав «нейтральное» уведомление», - сообщает Check Point. «В случае… приложения Cake VPN отображается уведомление «GooglePlayServices» без дополнительного текста».

Тем временем приложение ожидает команды от Firebase C2. Как только будет сказано запустить функцию loadAndInstallApp, полезная нагрузка будет загружена с GitHub. Затем он вызывает метод «installApp», чтобы завершить вредоносную активность.

Если зараженное устройство препятствует установке приложений из неизвестных источников, Clast82 предлагает пользователю поддельный запрос, выдавая себя за «Сервисы Google Play». Эти поддельные запросы будут появляться каждые пять секунд.

Зараженные приложения Clast 82 для Android

После того, как Check Point Research сообщила о своих выводах команде безопасности Android, Google подтвердил, что все приложения Clast82 были удалены из Google Play Store. Однако жертвы с уже установленными приложениями остаются в группе риска. Затронутые приложения следующие:

BeatPlayer

VPN

Две версии eVPN

Музыкальный проигрыватель

Тихоокеанский VPN

Сканер QR / штрих-кода MAX

QRecorder…» ***(Tara Seals. Google Play Harbors Malware-Laced Apps Delivering Spy Trojans // Threatpost (https://threatpost.com/google-play-malware-spy-trojans/164601/). 09.03.2021).***

***

«Исследователи безопасности в Intezer обнаружили ранее недокументированный бэкдор, получивший название RedXOR, со ссылками на спонсируемую Китаем хакерскую группу и используемый в продолжающихся атаках на системы Linux.

RedXOR образцы вредоносных программ найдены Intezer были загружены на VirusTotal (1, 2) из Тайваня и Индонезии (известные целей для китайских государственных хакеров) и имеет низкий уровень обнаружения.

Поскольку командно-управляющие серверы все еще активны, бэкдор Linux используется в продолжающихся атаках, нацеленных как на серверы Linux, так и на конечные точки.

RedXOR обладает большим набором возможностей, включая выполнение команд с системными привилегиями, управление файлами на зараженных компьютерах Linux, скрытие процесса с помощью руткита с открытым исходным кодом Adore-ng, проксирование вредоносного трафика, удаленное обновление и многое другое.

Ссылки на китайское вредоносное ПО Winnti

Новое вредоносное ПО считается новым вредоносным инструментом, добавленным в арсенал китайской зонтичной группы угроз Winnti.

«Основываясь на виктимологии, а также на аналогичных компонентах и тактиках, методах и процедурах (TTP), мы полагаем, что RedXOR был разработан известными китайскими злоумышленниками», - сказал Intezer.

Intezer также обнаружил множественные связи между бэкдором RedXOR Linux и множеством штаммов вредоносных программ, связанных с хакерами состояния Winnti, включая бэкдор PWNLNX и ботнеты Groundhog и XOR.DDOS.

Сходства, обнаруженные исследователями безопасности при сравнении этих вредоносных программ, включают использование:

старые руткиты ядра с открытым исходным кодом,

функции с одинаковыми названиями,

Вредоносный трафик в кодировке XOR,

сопоставимая схема именования для сервисов сохранения,

компиляция с использованием устаревших компиляторов Red Hat,

очень похожий поток кода и функциональность, и многое другое.

Кто такой Виннти?

Winnti - это общий термин, используемый для отслеживания коллектива поддерживаемых государством хакерских групп (BARIUM от Microsoft, APT41 от FireEye, Blackfly и Suckfly от Symantec, Wicked Panda от CrowdStrike), связанных с интересами правительства Китая.

Эти APT-группы имеют общий арсенал вредоносных инструментов, используемых для кибершпионажа и финансово мотивированных атак как минимум с 2011 года.

Именно тогда исследователи «Лаборатории Касперского» обнаружили троянскую программу Winnti на огромном количестве скомпрометированных игровых систем после атаки цепочки поставок, которая скомпрометировала официальный сервер обновлений игры.

Kaspersky также обнаружил доказательства, связывающие тактику атаки Winnti и методы, использованные при взломе ASUS LiveUpdate во время операции ShadowHammer, с теми, которые использовались в других атаках на цепочки поставок, включая NetSarang и CCleaner от 2017 года.

Группы APT все чаще нацелены на пользователей Linux

Обнаружение новых вредоносных программ совсем не удивительно, учитывая рост числа новых вредоносных программ для Linux более чем на 40% в течение 2020 года.

Национальные хакеры также все больше и больше сосредотачиваются на нацеливании на системы Linux, как подчеркивается в отчете Intezer за 2020 год, в котором подводятся итоги последних десяти лет атак Linux APT.

«В предыдущее десятилетие исследователи обнаружили несколько крупных APT-кампаний, нацеленных на системы Linux, а также уникальные вредоносные инструменты Linux, предназначенные для шпионских операций», - сказал Интезер.

«Некоторые из наиболее известных национальных государств включают в свой арсенал наступательные возможности Linux, и ожидается, что как количество, так и изощренность таких атак со временем будут расти». ***(Sergiu Gatlan. Chinese state hackers target Linux systems with new malware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/chinese-state-hackers-target-linux-systems-with-new-malware/). 11.03.2021).***

***

«Новый ботнет выслеживает и превращает зараженные маршрутизаторы, видеорегистраторы и сетевые устройства UPnP в приманки, которые помогают ему находить другие цели для заражения.

Вредоносная программа, названная ZHtrap обнаружившими ее исследователями безопасности 360 Netlab, основана на исходном коде Mirai и поддерживает архитектуры x86, ARM, MIPS и других процессоров.

Захватывает зараженные устройства

Как только он захватывает устройство, он предотвращает повторное заражение его ботов другими вредоносными программами с помощью белого списка, который разрешает только уже запущенные системные процессы, блокируя все попытки запуска новых команд.

Боты ZHtrap используют командно-административный сервер (C2) Tor для связи с другими узлами ботнета и прокси-сервер Tor для сокрытия вредоносного трафика.

Основные возможности ботнета включают DDoS-атаки и поиск более уязвимых устройств для заражения. Однако он также имеет функцию бэкдора, позволяющую операторам загружать и выполнять дополнительные вредоносные полезные данные.

Для распространения ZHtrap использует эксплойты, нацеленные на четыре N-дневные уязвимости безопасности в конечных точках Realtek SDK Miniigd UPnP SOAP, MVPower DVR, Netgear DGN1000 и длинном списке устройств CCTV-DVR.

Он также сканирует устройства со слабыми паролями Telnet из списка случайно сгенерированных IP-адресов и собирает их с помощью приманки, которую он развертывает на устройствах, уже подключенных к ботнету.

Боты, используемые как приманки

Самая интересная особенность ZHtrap - это то, как он превращает зараженные устройства в приманки для сбора IP-адресов большего количества

целей, которые могут быть уязвимы для его методов распространения или уже заражены другим вредоносным ПО.

После развертывания приманка ZHtrap начинает прослушивать список из 23 портов и отправляет все подключенные к ним IP-адреса в свой модуль сканирования в качестве потенциальных целей для своих атак.

«По сравнению с другими ботнетами, которые мы анализировали ранее, наиболее интересной частью ZHtrap является его способность превращать зараженные устройства в приманку», - сказал 360 Netlab.

«Ханипоты обычно используются исследователями безопасности в качестве инструмента для перехвата атак, таких как сбор сканированных изображений, эксплойтов и образцов.

«Но на этот раз мы обнаружили, что ZHtrap использует похожую технику, интегрируя модуль сканирования IP-адресов, и собранные IP-адреса используются в качестве целей в его собственном модуле сканирования»…». ***(Sergiu Gatlan. New ZHtrap botnet malware deploys honeypots to find more targets // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-zhtrap-botnet-malware-deploys-honeypots-to-find-more-targets/). 12.03.2021).***

***

«Действия вторжений, связанных с вредоносным ПО Supernova, установленным на скомпрометированных установках SolarWinds Orion, открытых в общедоступных интернет-ресурсах, указывают на злоумышленника из Китая.

Исследователи безопасности назвали группу хакеров Spiral и сопоставили результаты двух вторжений в 2020 году в одну и ту же сеть жертв, чтобы определить активность одного и того же злоумышленника.

В отличие от вредоносного ПО, использованного в атаке цепочки поставок SolarWinds [1, 2, 3], которое было встроено в сборки программного обеспечения Orion от разработчика, веб-оболочка Supernova закрылась внутри платформы после того, как хакеры использовали критическую уязвимость в установках продукта, доступную через общедоступная сеть.

Первоначальная оценка пришла к выводу, что вредоносное ПО принадлежит к другой группе угроз, нежели Nobelium, поскольку Microsoft отслеживает хакеров цепочки поставок, связанных с Россией. Другие отслеживают актера под разными именами: UNC2452 (FireEye), StellarParticle (CrowdStrike), SolarStorm (Palo Alto Networks), Dark Halo (Volexity).

Многолетняя настойчивость

Исследователи SecureWorks Counter Threat Unit (CTU) обнаружили, что Supernova упала в сеть клиента во время работы по реагированию на инциденты в ноябре 2020 года.

Вектор вторжения - обход аутентификации SolarWinds Orion API (CVE-2020-10148), который позволил злоумышленнику выполнить сценарий и команды разведки и сбросить веб-оболочку Supernova через 30 минут.

Промежуток между последней командой разведки и удалением веб-оболочки, вероятно, объясняется тем, что злоумышленник запускает сканирование и эксплойт и находит дорогостоящие жертвы в сети.

Атака была целевой, потому что после установки веб-оболочки злоумышленник сопоставил сетевые ресурсы только на двух серверах, что дало им контроль над доменом и доступ к конфиденциальным бизнес-данным.

После установки Supernova в SolarWinds Orion путем троянизации легитимного файла, который использовала платформа (app_web_logoimagehandler.ashx.b6031896.dll), злоумышленник использовал библиотеку comsvcs.dll для сброса содержимого процесса LSASS (Служба подсистемы локального органа безопасности).

Более раннее вторжение в ту же сеть, выявленное в августе, было осуществлено аналогичным образом, но точкой входа был уязвимый общедоступный сервер ManageEngine ServiceDesk.

В этом случае SecureWorks CTU обнаружил, что первоначальный доступ произошел в 2018 году, и хакеры «использовали доступ для периодического сбора и эксфильтрации учетных данных домена».

В то время исследователям не удалось отнести активность к конкретной группе угроз, но они заметили, что использовали тот же метод и путь к выходному файлу для дампа процесса LSASS,

Однако на этом сходство не ограничилось, поскольку актер получил доступ к тем же двум серверам, что и во время инцидента в ноябре 2020 года. Кроме того, в обоих случаях использовались три скомпрометированных учетных записи администратора.

Ссылка на Китай

Хотя методы работы (нацеливание на серверы ManageEngine, долгосрочное упорство для сбора учетных данных и кражи данных, кража интеллектуальной собственности) характерны для китайских хакерских групп, он не считается убедительным доказательством более надежной атрибуции.

Однако вторжение в августе предоставило исследователям более надежную деталь для подтверждения их теории: IP-адрес в Китае для хоста в инфраструктуре злоумышленника.

«Соглашение об именах этого хоста было таким же, как у другого хоста, используемого злоумышленником для подключения к сети через соединение VPN» SecureWorks CTU

Основываясь на своем анализе, исследователи SecureWorks CTU полагают, что хакеры, вероятно, раскрыли IP-адрес после того, как они загрузили установщик агента конечной точки из сети и установили его в своей инфраструктуре.

«Раскрытие IP-адреса, вероятно, было непреднамеренным, поэтому его геолокация подтверждает гипотезу о том, что группа угроз SPIRAL действует за пределами Китая», - говорят исследователи.

Исследователи подчеркивают трудности приписывания кибератак конкретному злоумышленнику, но полагают, что их открытия указывают на находящуюся в Китае хакерскую бригаду.

Они предоставляют набор индикаторов взлома, содержащий IP-адреса для инфраструктуры Spiral в Китае и серверов управления и контроля, а также хэши для веб-оболочки Supernova, полученные после использования CVE-2020-10148.

Обновление [8 марта, 19:28 по восточному времени]: SolarWinds обратилась к BleepingComputer с заявлением, чтобы уточнить, что Supernova - это вредоносное ПО, внедренное в программное обеспечение Orion в клиентской сети, а не часть атаки цепочки поставок, приписываемой российским хакерам.

«В этом отчете упоминается инцидент, когда сеть впервые взломана способом, не была использована с SolarWinds. Это нарушение нарушено злоумышленникам вредоносный код Supernova в программное обеспечение Orion в сети клиента. Важно отметить, что Supernova не связана с широкой и сложной атакой цепочки поставок, нацеленной на несколько компаний-разработчиков программного обеспечения в качестве векторов. Supernova не была подписана и не доставлена SolarWinds, и проблема была решена в обновлениях платформы Orion, выпущенных в декабре»- SolarWinds». ***(Ionut Ilascu. Hackers hiding Supernova malware in SolarWinds Orion linked to China // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-hiding-supernova-malware-in-solarwinds-orion-linked-to-china/). 08.03.2021).***

***

«Вредоносная программа TrickBoot может получить возможность чтения, записи и удаления прошивок, если на устройстве отключена защита от записи UEFI/BIOS.

Компании Supermicro и Pulse Secure выпустили предупреждения, что некоторые из их материнских плат уязвимы к модулю заражения прошивок UEFI вредоносного ПО TrickBot, известного как TrickBoot.

Напомним, в прошлом году в совместном отчете специалисты из Advanced Intelligence (AdvIntel) и Eclypsium, представили технические подробности нового компонента TrickBot. TrickBoot — средство разведки, проверяющее наличие уязвимостей в прошивке UEFI зараженного устройства. В настоящее время способность вредоносного ПО анализировать прошивку устройства ограничена конкретными платформами Intel (Skylake, Kaby Lake, Coffee Lake, Comet Lake).

Новый модуль проверяет, активна ли защита от записи UEFI/BIOS, с помощью драйвера RwDrv.sys от RWEverything (бесплатная утилита, обеспечивающая доступ к аппаратным компонентам). Если защита отключена, вредоносная программа получает возможность чтения, записи и удаления прошивок. Таким образом вредонос может блокировать устройство, обходить средства контроля безопасности операционной системы или повторно заражать систему даже после полной переустановки.

Представители Supermicro предупредили, что некоторые из материнских плат X10 UP уязвимы к вредоносному ПО TrickBoot, и выпустили обновление BIOS для включения защиты от записи. Supermicro выпустила версию BIOS 3.4 для устранения уязвимости, но публично выпустила ее только для материнской платы X10SLH-F.

Уязвимые материнские платы серии X10 UP («Denlow») включают X10SLH-F, X10SLL-F, X10SLM-F, X10SLL+-F, X10SLM+-F, X10SLM+-LN4F, X10SLA-F, X10SL7-F, X10SLL-S/-S. Владельцы материнских плат, достигших срока окончания поддержки (End of Life, EOL), должны связаться с Supermicro, чтобы получить доступ к новому BIOS.

Pulse Secure также выпустила рекомендации, поскольку устройства Pulse Secure Appliance 5000 (PSA-5000) и Pulse Secure Appliance 7000 (PSA-7000) работают на уязвимом оборудовании Supermicro. В настоящее время Pulse Secure выпустила исправление BIOS для устройств, работающих под управлением Pulse Connect Secure или Pulse Policy Secure. Pulse Secure предупреждает, что для установки патча потребуется перезагрузка устройства». ***(Supermicro и Pulse Secure выпустили патчи для защиты от атак TrickBoot // SecurityLab.ru (https://www.securitylab.ru/news/517173.php). 05.03.2021).***

***

«Вредоносные Xcode projects использовали, чтобы «угнать» системы разработчиков и распространить бэкдор EggShell.

Малварь XcodeSpy атакует Xcode – интегрированную среду разработки (ИСР), которая используется в macOS для разработки ПО и приложений на Apple.

Согласно исследованию SentinelLabs, функцию Run Script в ИСР использовали для атаки на разработчиков iOS. Для этого использовали троянские проекты Xcode.

Проекты Xcode можно найти на GitHub. Проекты XcodeSpy предлагают «расширенный функционал» для анимации панелей вкладок iOS – и как только сборка скачана и запущена, развертывается вредоносный код, чтобы установить бэкдор EggShell.

Run Script в ИСР незаметно подделали, чтобы подключить сервер управления и контроля (C2) злоумышленника к проекту разработчика. В частности, хакеры использовали функционал ИСР Apple, который позволяет развертывать пользовательские shell-скрипты при запуске экземпляра приложения.

Бэкдор способен «угнать» микрофон, камеру и клавиатуру жертвы, а также отправить файлы на C2 злоумышленника.

Жертвами такой атаки стали по крайней мере одна компания в США, а также некоторые разработчики Азии.

Кампания длилась с июля по октябрь 2020 года». ***(Разработчиков Apple атаковали новой малварью – бэкдором EggShell // SecureNews (https://securenews.ru/apple-developers-were-attacked-by-a-new-malware-the-eggshell-backdoor/). 18.03.2021).***

***

«Модернизированный вариант вредоносного ПО Purple Fox с возможностями червя развертывается в рамках кампании атаки, которая быстро расширяется.

Purple Fox, впервые обнаруженная в 2018 году, представляет собой вредоносное ПО, которое использовалось для распространения с помощью наборов

эксплойтов и фишинговых писем. Однако новая кампания, проводимая в последние несколько недель и которая продолжается, выявила новый метод распространения, ведущий к высокому числу заражений.

В сообщении в блоге во вторник Guardicore Labs сообщила, что Purple Fox теперь распространяется посредством «неизбирательного сканирования портов и эксплуатации уязвимых сервисов SMB со слабыми паролями и хешами».

По данным телеметрии Guardicore Global Sensors Network (GGSN), активность Purple Fox начала расти в мае 2020 года. Хотя с ноября 2020 года по январь 2021 года было затишье, исследователи говорят, что общее число заражений выросло примерно на 600%, а общее количество атак в настоящее время сохраняется. на 90 000.

Вредоносная программа нацелена на компьютеры Microsoft Windows и перепрофилирует скомпрометированные системы для размещения вредоносных полезных нагрузок. Guardicore Labs заявляет, что на «мешанине уязвимых и эксплуатируемых серверов» размещается исходная полезная нагрузка вредоносного ПО, многие из которых работают под управлением более старых версий Windows Server с Internet Information Services (IIS) версии 7.5 и Microsoft FTP.

Цепочки заражения могут начинаться через службы с выходом в Интернет, содержащие уязвимости, такие как SMB, эксплойты браузера, отправленные с помощью фишинга, атаки методом перебора или развертывание с помощью руткитов, включая RIG.

На данный момент операторы ботнета Purple Fox захватили около 2000 серверов.

Исследователи Guardicore Labs говорят, что после того, как выполнение кода на целевой машине достигнуто, для управления персистентностью необходимо создать новую службу, которая зацикливает команды и извлекает полезные данные Purple Fox из вредоносных URL-адресов.

Установщик вредоносного ПО MSI маскируется под пакет Центра обновления Windows с разными хэшами. Команда называет эту функцию «дешевым и простым» способом избежать подключения установщиков вредоносного ПО друг к другу во время расследования.

В общей сложности затем извлекаются и дешифруются три полезной нагрузки. Один из них вмешивается в возможности брандмауэра Windows, и создаются фильтры для блокировки ряда портов - потенциально в попытке предотвратить повторное заражение уязвимого сервера другим вредоносным ПО.

Интерфейс IPv6 также устанавливается для сканирования портов и «максимизации эффективности распространения по (обычно не отслеживаемым) подсетям IPv6», отмечает группа, перед загрузкой руткита и перезапуском целевой машины. Purple Fox загружается в системную DLL для выполнения при загрузке.

Затем Purple Fox сгенерирует диапазоны IP-адресов и начнет сканирование порта 445 для распространения.

«Когда машина отвечает на зонд SMB, отправляемый через порт 445, он будет пытаться аутентифицироваться в SMB путем подбора имен пользователей и паролей или путем попытки установить нулевой сеанс», - говорят исследователи.

Программа установки трояна / руткита использует стеганографию, чтобы скрыть локальные двоичные файлы повышения привилегий (LPE) в прошлых атаках.

Индикаторы компрометации (IoC) опубликованы на GitHub». ***(Charlie Osborne. Purple Fox malware evolves to propagate across Windows machines // ZDNet (https://www.zdnet.com/article/purple-fox-malware-evolves-to-propagate-across-windows-machines/). 24.03.2021).***

***

«Исследователи безопасности говорят, что новое мощное вредоносное ПО для Android, маскирующееся под критическое обновление системы, может получить полный контроль над устройством жертвы и украсть ее данные.

Вредоносное ПО было обнаружено в приложении под названием «Обновление системы», которое необходимо было установить вне Google Play, магазина приложений для устройств Android. После установки пользователем приложение скрывает и незаметно пересылает данные с устройства жертвы на серверы оператора.

Исследователи из компании по обеспечению безопасности мобильных устройств Zimperium, обнаружившей вредоносное приложение, заявили, что после того, как жертва установит вредоносное приложение, вредоносное ПО связывается с сервером Firebase оператора, который используется для удаленного управления устройством.

Шпионское ПО может красть сообщения, контакты, сведения об устройстве, закладки браузера и историю поиска, записывать звонки и окружающий звук с микрофона, а также делать фотографии с помощью камер телефона. Вредоносная программа также отслеживает местоположение жертвы, ищет файлы документов и захватывает скопированные данные из буфера обмена устройства.

Вредоносная программа скрывается от жертвы и пытается избежать захвата, уменьшая объем потребляемых сетевых данных, загружая на серверы злоумышленника эскизы, а не полное изображение. Вредоносная программа также собирает самые свежие данные, включая местоположение и фотографии.

Генеральный директор Zimperium Шридхар Миттал сказал, что вредоносная программа, скорее всего, была частью целевой атаки.

«Это, пожалуй, самое сложное, что мы когда-либо видели», - сказал Миттал. «Я думаю, что на создание этого приложения было потрачено много времени и усилий. Мы считаем, что существуют и другие подобные приложения, и изо всех сил стараемся найти их как можно скорее».

Обманом заставить кого-то установить вредоносное приложение - простой, но эффективный способ скомпрометировать устройство жертвы. Вот почему устройства Android предупреждают пользователей о том, что нельзя устанавливать приложения из-за пределов магазина приложений. Но многие старые устройства не запускают последние приложения, что вынуждает пользователей полагаться на более старые версии своих приложений из нелегальных магазинов приложений.

Миттал подтвердил, что вредоносное приложение никогда не устанавливалось в Google Play. По сообщению, представитель Google не стал

комментировать, какие шаги компания предпринимала для предотвращения попадания вредоносного ПО в магазин приложений Android. Google и раньше видел, как вредоносные приложения проскальзывают через его фильтры.

Этот вид вредоносного ПО имеет широкий доступ к устройству жертвы и имеет множество форм и названий, но в основном делает то же самое. На заре Интернета трояны удаленного доступа, или RAT, позволяли шпионам шпионить за жертвами через их веб-камеры. В настоящее время приложения для наблюдения за детьми часто перепрофилируются для слежки за супругом человека, что называется сталкерским или spouseware.

В прошлом году TechCrunch сообщил о сталкерском ПО KidsGuard - якобы приложение для наблюдения за детьми - которое использовало аналогичное «обновление системы» для заражения устройств жертв.

Но исследователи не знают, кто создал вредоносное ПО и на кого оно нацелено.

«Мы начинаем видеть рост числа RAT на мобильных устройствах. И уровень сложности, похоже, повышается, похоже, что злоумышленники осознали, что мобильные устройства содержат столько же информации и гораздо менее защищены, чем традиционные конечные точки», - сказал Миттал». ***(Zack Whittaker. A new Android spyware masquerades as a 'system update' // Verizon Media (https://techcrunch.com/2021/03/26/android-malware-system-update/). 26.03.2021).***

***

«В 2020 году обнаружение бесфайловых малварей выросло почти на 900%, согласно отчету Watchguard Technologies.

Количество бесфайловых малварей выросло за год на 888%, так как злоумышленники стремились скрыться от программ для защиты устройства. Они проводили атаки без установки вредоносного кода.

Были популярны такие наборы инструментов, как PowerSploit и CobaltStrike. С их помощью хакеры внедряли вредоносный код в запущенные процессы так, чтобы в случае обнаружения и удаления скрипта, они оставались в рабочем состоянии.

Также, как сообщает Watchguard, 47% из всех атак были обнаружены зашифрованными. Количество вредоносного ПО, поставляемого через HTTPS, выросло на 41%, а количество зашифрованных ошибок нулевого дня – на 22%.

Компания также обнаружила на 25% больше малварей для добычи криптовалюты в 2020 по сравнению с 2019». ***(Обнаружение бесфайловых малварей выросло почти на 900% в 2020 // SecureNews (https://securenews.ru/detection-of-file-free-malware-increased-by-almost-900-in-2020/). 30.03.2021).***

***

«…ФБР предупредило о росте атак программ-вымогателей PYSA на образовательные учреждения в США и Великобритании.

В прошлом году власти Великобритании и Франции также выпустили предупреждения о программе-вымогателе PYSA после атак на правительственные и другие типы организаций.

По данным ФБР, атаки PYSA были организованы «неустановленными киберпреступниками» против высших учебных заведений, школ и семинарий K-12 в десятке штатов США, а также Великобритании.

Известно, что злоумышленники, стоящие за атаками PYSA, шифруют данные в скомпрометированных системах и также крадут информацию у жертв, угрожая их утечкой, чтобы повысить свои шансы на получение оплаты.

PYSA, также известная как Mespinoza, существует как минимум с октября 2019 года, а ФБР отслеживает ее с марта 2020 года. Атаки программ-вымогателей PYSA наблюдались против правительственных организаций, образовательных учреждений, сектора здравоохранения и частного бизнеса.

Злоумышленники часто используют фишинг и атаки RDP для первоначального доступа к целевым сетям, а затем используют такие инструменты, как Advanced Port / IP Scanner, PowerShell Empire, Mimikatz и Koadic, чтобы получить дополнительный доступ.

После извлечения потенциально ценных файлов из сети жертвы, зачастую содержащей записи о занятости и финансовую информацию, киберпреступники шифруют файлы на устройствах Windows и Linux.

Предупреждение ФБР содержит некоторую техническую информацию об этих атаках, а также индикаторы компрометации (IoC). Агентство посоветовало организациям не платить, но отметило, что «понимает, что, когда жертвы сталкиваются с неспособностью функционировать, оцениваются все варианты с целью защиты акционеров, сотрудников и клиентов».

Жертвам атак программы-вымогателя PYSA рекомендовано направить отчет в ФБР.

«Образовательные учреждения - большие мишени для хакеров, поскольку потенциально может быть задействована конфиденциальная информация тысяч людей, а существенный переход на электронное обучение сделал их еще более привлекательными для хакеров и программ-вымогателей», - сказал SecurityWeek Джеймс Кардер, CSO LogRhythm. «Эти атаки на школы могут привести к остановке образования, потенциально раскрывая личные данные каждого ученика и учителя в организации. Родители также становятся жертвами и могут быть вынуждены заплатить выкуп за личную информацию или школьные задания, если информация попадет в руки злоумышленников»…». ***(Eduard Kovacs. FBI Warns of PYSA Ransomware Attacks on Education Institutions in US, UK // Wired Business Media (https://www.securityweek.com/fbi-warns-pysa-ransomware-attacks-education-institutions-us-uk?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Securityweek+%28SecurityWeek+RSS+Feed%29). 17.03.2021).***

***

«…Исследователи кибербезопасности из Palo Alto Networks проанализировали атаки программ-вымогателей, нацеленных на организации в Северной Америке и Европе, и обнаружили, что средний выкуп, выплачиваемый в обмен на ключ дешифрования для разблокировки зашифрованных сетей, вырос со 115 123 долларов в 2019 году до 312 493 долларов в 2020 году.

Это на 171 процент больше, чем за год, что позволяет киберпреступникам зарабатывать больше денег, чем когда-либо прежде, на атаках программ-вымогателей.

Программы-вымогатели остаются эффективным инструментом для киберпреступников, поскольку многие организации по-прежнему плохо оснащены для борьбы с угрозой, что приводит к тому, что многие жертвы уступают требованиям вымогательства и платят выкуп в биткойнах в надежде получить ключ дешифрования, необходимый для восстановления их сети.

Этому способствовало появление дополнительных тактик вымогательства, например, когда киберпреступники шифруют и крадут данные, угрожая жертве опубликовать украденную информацию, если выкуп не будет уплачен. В некоторых случаях это приводит к тому, что организации, которые могут восстановить сеть без уплаты выкупа, в любом случае становятся жертвами шантажа…

Наибольший спрос на выкуп в течение 2020 года составил 30 миллионов долларов, что вдвое превышает предыдущий самый высокий уровень спроса в 15 миллионов долларов в предыдущие годы.

А учитывая постоянный успех атак программ-вымогателей - и появление новых успешных вариантов программ-вымогателей и простых в использовании схем «программа - вымогатель как услуга» - маловероятно, что киберпреступники замедлят свою работу в ближайшее время.

«Программы-вымогатели - одна из главных угроз кибербезопасности», - сказал Джон Дэвис, вице-президент по государственному сектору Palo Alto Networks…

Вымогатели группа, включая Ryuk, Эгрегор, DoppelPaymer и многие другие продолжает досаждать организации по всему миру в 2021 году, но при правильной стратегии кибербезопасности, можно защитить от атак…». ***(Danny Palmer. Largest ransomware demand now stands at $30 million as crooks get bolder // ZDNet (https://www.zdnet.com/article/largest-ransomware-demand-now-stands-at-30-million-as-crooks-get-bolder/). 17.03.2021).***

***

«Федеральное правительство предоставило рекомендации о том, как противодействовать программам-вымогателям в Австралии, поощряя использование многофакторной аутентификации и призывая предприятия поддерживать программное обеспечение в актуальном состоянии, архивировать данные и резервное копирование, встраивать функции

безопасности в системы и обучать сотрудников эффективной кибербезопасности. гигиена.

Совет был дан в документе Locked Out: Tackling Australia's ransomware угрозы, который представляет собой 14-страничный документ [PDF], подготовленный Консультативным комитетом индустрии кибербезопасности. Министерство внутренних дел рекламирует его как «[повышение] осведомленности всех австралийцев и их предприятий о текущем ландшафте угроз вымогателей».

«Атаки программ-вымогателей сегодня представляют серьезную угрозу для австралийских организаций», - говорится в сообщении. «В 2020 году киберпреступники провели успешные атаки на крупные австралийские организации в невиданных ранее объемах».

В документе представлены тематические исследования атак, таких как та, которую испытал Toll в прошлом году, а также даны советы о том, как защититься от атак программ-вымогателей.

«Раннее обнаружение атаки программ-вымогателей имеет первостепенное значение для минимизации воздействия», - говорится в сообщении.

В нем также говорится, что многих из наиболее эффективных атак с использованием программ-вымогателей можно было бы избежать с помощью основных средств контроля кибербезопасности и надлежащей гигиены кибербезопасности.

«Для малых предприятий, которые составляют 93% занятых в Австралии предприятий и обеспечивают работой почти 45% рабочей силы Австралии, проблема в другом», - продолжил он.

«У них нет начальников службы безопасности, ИТ-команды или, возможно, даже квалифицированного ИТ-члена, что понятно, когда более половины сотрудников нанимают менее четырех человек.

«У всех предприятий есть ценные данные и системы, которые они должны защищать. Жизненно важно, чтобы они установили надежный фундаментальный контроль и применяли надлежащие методы гигиены кибербезопасности».

Затем статья указала читателям на не столь важные элементы управления Essential Eight для предотвращения кибератак Австралийского центра кибербезопасности (ACSC).

В статье говорится, что организациям следует рассматривать киберстрахование как один из компонентов целостной программы кибербезопасности, а не как замену ему.

В прошлом месяце два члена теневого министерства труда призвали к разработке национальной стратегии в отношении программ-вымогателей, направленной на сокращение числа таких атак на цели в Австралии. Теневой министр внутренних дел Кристина Кенелли и теневой помощник министра связи Тим Уоттс заявили, что из-за того, что программы-вымогатели являются самой большой угрозой для Австралии, пришло время разработать стратегию, чтобы предотвратить их.

В четверг Уоттс назвал правительственную газету о вымогателях упущенной возможностью.

«Хотя лейбористы приветствуют признание правительством проблемы программ-вымогателей, в этом отчете не отражается масштаб проблемы в 1 миллиард австралийских долларов», - сказал он.

«Вместо того, чтобы использовать возможность начать дебаты о роли, которую правительство может сыграть в формировании исчисления банд вымогателей, оценивающих австралийские организации, правительство Моррисона продолжает свой подход, основанный на игре в поиски виноватых».

По мнению Уоттса, недостаточно говорить бизнесу, чтобы тот защищался, «запирая двери для киберпреступных банд».

«Как предупредил Австралийский центр кибербезопасности, банды вымогателей используют все более изощренные организационные модели и тактику давления, чтобы получить рекордную незаконную прибыль», - сказал он.

Такой ответ, по словам Уоттса, особенно разочаровал перед лицом поддерживаемой государством кампании Hafnium против серверов Microsoft Exchange.

«Тысячи австралийских серверов потенциально уязвимы для новой волны атак программ-вымогателей, использующих эту уязвимость и потенциально разрушающих финансовые дела австралийских предприятий», - продолжил Уоттс. «Правительство Моррисона должно делать больше для активного противодействия угрозе программ-вымогателей и разработки национальной стратегии в отношении программ-вымогателей».

После взлома Microsoft Exchange Server помощник министра обороны Эндрю Хасти в среду обратился к австралийским организациям с просьбой предпринять немедленные шаги по срочному исправлению уязвимых систем.

«ACSC выявила большое количество австралийских организаций, которые еще не исправили уязвимые версии Microsoft Exchange, что делает их уязвимыми для киберкомпрометации», - сказал Хасти.

«Австралийские организации не могут останавливаться на достигнутом, когда дело касается кибербезопасности, поэтому всех пользователей Microsoft Exchange призывают исправить свои уязвимые системы».

Уоттс назвал ответ правительства отложенным…». ***(Asha Barbaschow. Australia's answer to thwarting ransomware is good cyber hygiene // ZDNet (https://www.zdnet.com/article/australias-answer-to-thwarting-ransomware-is-good-cyber-hygiene/). 11.03.2021).***

***

«Две недавно обнаруженные формы программ-вымогателей с очень разными характеристиками показывают, насколько разнообразным стал мир программ-вымогателей по мере того, как все больше преступников пытаются присоединиться к кибер-вымогательству.

Обе формы программ-вымогателей появились в феврале и были подробно описаны исследователями кибербезопасности из Trend Micro - AlumniLocker и Humble - с двумя версиями, пытающимися вымогать выкуп в биткойнах по-разному.

AlumniLocker - это вариант программы-вымогателя Thanos, который сразу же выделяется тем, что требует от зараженной жертвы выплаты 10 биткойнов - в настоящее время эта цифра эквивалентна примерно 450 000 долларов.

Программа-вымогатель доставляется жертвам через вредоносное вложение в формате PDF, которое представляет собой счет-фактуру, распространяемую в фишинговых письмах. PDF-файл содержит ссылку, по которой будет извлечен ZIP-архив, который запускает сценарий PowerShell для удаления полезной нагрузки и запуска программы-вымогателя.

Подобно растущему числу кампаний вымогателей, злоумышленники, стоящие за AlumniLocker, угрожают опубликовать данные, украденные из сети их жертвы, если им не заплатят в течение 48 часов - хотя, учитывая, что требования выкупа настолько велики, жертвы могут решить, что платить слишком много.

Амбициозное требование выкупа и другие несоответствия в их методах атаки, в том числе то, что сайт утечки данных на самом деле не работает, могут указывать на то, что те, кто стоит за AlumniLocker, вероятно, только начинают.

«Похоже, что это может быть новая группа, у которой нет опыта успешного выкупа своих жертв, поскольку требования выкупа намного выше, чем обычно. То, что сайт утечки не работает, - еще один пример того, как показать свою руку новичков. ", - сказал ZDNet Джон Клэй, директор по глобальным коммуникациям Trend Micro.

Программа-вымогатель Humble также впервые появилась в феврале, но во многих отношениях она сильно отличается. Во-первых, программа-вымогатель намного меньше по размеру и требует всего 0,0002 биткойна - в настоящее время чуть менее 10 долларов - для возврата файлов, что указывает на то, что Humble может быть нацелен на отдельных лиц, а не на организации.

Пока неизвестно, как именно распространяется Humble, но исследователи отмечают, что это может быть через фишинговые атаки.

Пытаясь подтолкнуть жертв к уплате выкупа, Хамбл угрожает жертве, заявляя, что если они перезапустят свою систему, основная загрузочная запись (MBR) будет перезаписана, что сделает машину непригодной для использования. Вторая версия Humble несет в себе ту же угрозу, но вместо этого говорит, что это произойдет, если жертва не заплатит через пять дней.

Humble необычен для программ-вымогателей тем, что он скомпилирован с исполняемой оболочкой (Bat2Exe) в пакетном файле. Что еще странно, так это то, что он использует Discord - сервис голосовой, текстовой и видеосвязи, популярный среди геймеров, - чтобы отправлять отчеты своему автору.

Обе формы новых программ-вымогателей необычны, но обе демонстрируют, что программы-вымогатели продолжают привлекать киберпреступников, которые видят, как ведущие банды зарабатывают так много денег, и хотят делать то же самое.

Организации могут помочь защитить себя от атак программ-вымогателей с помощью процедур кибербезопасности, включая применение исправлений и использование многофакторной аутентификации». ***(Danny Palmer. These two unusual versions of ransomware tell us a lot about how attacks are evolving // ZDNet***

(https://www.zdnet.com/article/these-two-unusual-versions-of-ransomware-tell-us-a-lot-about-how-attacks-are-evolving/). 05.03.2021).

***

«Агентство, отвечающее за управление пособиями по безработице в Испании, пострадало от программы-вымогателя Ryuk.

Испанская государственная служба занятости (SEPE) в Испании подверглась кибератаке, в результате чего были приостановлены ее системы связи в сотнях офисов и отложены встречи с тысячами.

SEPE - это «автономный орган» в Испании, который управляет и контролирует пособия по безработице. Кибератака произошла в и без того напряженное время для агентства, которое имеет дело с переполнением запросов на пособие по безработице, поскольку пандемия коронавируса вынудила компании по всему миру сократить свою рабочую силу.

По данным испанского профсоюза Central Sindical Independiente y de Funcionarios (CSIF), атака затронула 710 офисов организации. Профсоюз заявил, что кибератака была вызвана программой-вымогателем, однако дальнейшие подробности атаки, включая ее происхождение и требование выкупа, неизвестны.

«SEPE подвергается опасному инциденту, во время которого была нарушена доступность его информационных и коммуникационных систем», - говорится в сообщении на веб-сайте SEPE. «Первые неотложные действия были предприняты как можно быстрее и с основной целью сдержать инцидент, изолировать и, следовательно, смягчить его влияние на системы SEPE».

Согласно Business Insider Spain, кибератака была произведена программой - вымогателем Ryuk. Группа угроз за последний год поразила ряд организаций, например, Universal Health Services.

SEPE заявила, что все еще работает над обработкой запросов на пособие по безработице вручную, и нет необходимости возобновлять запросы.

Однако CSIF утверждает, что SEPE несколько месяцев медлит с инвестициями в технологии и полагается на приложения и компьютерные системы со «средним возрастом около 30 лет».

«В CSIF мы сожалеем о сбоях, которые эта проблема вызывает у пользователей и которые должным образом проинформированы об инциденте», - сообщает CSIF.

Такие эксперты, как Джигар Шах, вице-президент Valtix, сказали, что организациям необходимо быть «дальновидными», когда речь идет о защите своей инфраструктуры и отражении угроз программ-вымогателей.

«Многие люди слишком сосредоточены на тактических ответах после инцидента с вымогателем», - сказал Шах. «Часто выплата выкупа даже не позволяет вам восстановиться, поскольку злоумышленник просто исчезает и не помогает освободить заблокированные ресурсы. На данный момент большие затраты связаны с тем, чтобы восстановить и отстроить заново»…». ***(Lindsey O'Donnell. Ransomware Attack Strikes Spain's Employment Agency // Threatpost (https://threatpost.com/ransomware-attack-spain-employment-agency/164703/). 11.03.2021).***

***

«Многонациональная пивоваренная компания не сообщила, какой тип инцидента привел к «отключению системы», но она расследует и работает, чтобы вернуть сети в рабочее состояние.

Известная компания подверглась кибератаке, которая нанесла серьезный ущерб ее бизнесу. Пивоваренная компания Molson Coors признала в четверг, что у нее «произошел сбой системы, вызванный инцидентом кибербезопасности», согласно форме 8-K, поданной в SEC.

Компания не сообщила, какой тип атаки вызвал серьезные проблемы во всем ее бизнесе, включая операции пивоваренного завода, производство и поставки, но, учитывая недавние крупные атаки на другие основные компании, эксперты по безопасности предполагают, что это могла быть атака с использованием вымогателей.

Molson Coors наняла судебные ИТ-компании и юрисконсульта для расследования и «работает круглосуточно, чтобы восстановить свои системы как можно быстрее», говорится в заяве.

Возможная атака программ-вымогателей

«Громкие атаки становятся все более распространенными, поскольку злоумышленники осознали, что они намного более прибыльны, когда нацелены на крупные организации и нарушают их критически важные бизнес-операции - в данном случае пивоваренные операции крупнейших и известных пивных брендов в мире, - заметил Эдгард Капдевилль, генеральный директор Nozomi Networks.

Хотя компания не раскрыла конкретных подробностей инцидента, учитывая серьезность нарушения и недавнюю активность кибератак, «это могла быть программа-вымогатель», - сказал он.

Тони Ламберт, аналитик разведки Red Canary, отметил, что влияние программ-вымогателей на такие операции, как Molson Coors, может быть гораздо более разрушительным, чем для других видов предприятий.

Ситуацию такого типа следует учитывать в планах реагирования на инциденты и обеспечения непрерывности бизнеса, добавил Капдевилль: «Помимо технического реагирования, лица, принимающие решения, должны быть готовы взвесить риски и последствия альтернативных действий».

Атаки программ-вымогателей увеличатся в 2021 году

В последнее время активно действуют несколько групп программ-вымогателей, жертвами которых стали несколько крупных организаций, которые пострадали из-за атак.

Несколько из этих атак с использованием программ-вымогателей произошло только за последний месяц. Например, Государственная служба занятости Испании (SEPE) недавно подверглась атаке программы-вымогателя Ryuk, в результате которой были приостановлены ее системы связи в сотнях офисов и отложены встречи с тысячами. А в феврале Kia Motors была остановлена атакой программы-вымогателя, которую взяли на себя известные злоумышленники DoppelPaymer.

В том же время, WestRock - вторая по величине компания в США, которая рассчитывает на General Motors, Heinz и Home Depot в качестве клиентов - также подверглась нападениям в феврале, как и финский ИТ-гигант TietoEVRY.

Известные группы программ-вымогателей, которые были связаны с недавними атаками, включают вышеупомянутые DoppelPaymer и Ryuk; вымогатели Clop, которые были связаны с недавними глобальными атаками нулевого дня на пользователях Accellion Appliance; и HelloKitty, который, как подозревают, стоит за атакой CD Projekt Red - компании по разработке видеоигр, стоящей за Cyberpunk 2077, - которая также произошла в феврале.

Другой потенциальный виновник атаки Molson Coors может быть связан с атаками китайских и других групп устойчивых угроз повышенной сложности (APT) на недавно исправленные уязвимости Microsoft Exchange. Недостатки подвергаются критике со стороны как минимум 10 различных APT, все из которых сосредоточены на взломе почтовых серверов по всему миру, а исследователи наблюдают снежный ком активности эксплуатации.

Чтобы избежать кибератак, приводящих к остановке всех операций и серьезным сбоям в работе бизнеса, Кэпдевилль внес ряд рекомендаций по передовой практике кибербезопасности, включая сильную сегментацию, обучение пользователей, проактивные программы кибергигиены, многофакторную аутентификацию и использование постоянно обновляемой аналитики угроз». ***(Elizabeth Montalbano. Molson Coors Cracks Open a Cyberattack Investigation // Threatpost (https://threatpost.com/molson-coors-cyberattack-investigation/164722/). 12.03.2021).***

***

«Злоумышленники теперь устанавливают новую программу-вымогатель под названием DEARCRY после взлома серверов Microsoft Exchange с использованием недавно обнаруженных уязвимостей ProxyLogon.

Поскольку ранее в этом месяце Microsoft сообщила, что злоумышленники скомпрометировали серверы Microsoft Exchange с помощью новых уязвимостей нулевого дня ProxyLogon, серьезную озабоченность вызывает то, что злоумышленники будут использовать его для развертывания программ-вымогателей.

К сожалению, сегодня наши опасения стали реальностью, и злоумышленники используют уязвимости для установки программы-вымогателя DearCry.

Атаки начались 9 марта

По словам Майкла Гиллеспи, создателя сайта идентификации программ-вымогателей ID-Ransomware, начиная с 9 марта пользователи начали отправлять в его систему новое уведомление о выкупе и зашифрованные файлы.

Изучив представленные материалы, Гиллеспи обнаружил, что пользователи отправляли почти все из них с серверов Microsoft Exchange.

9 марта жертва также создала тему на форумах BleepingComputer, в которой они заявили, что их сервер Microsoft Exchange был скомпрометирован с использованием уязвимостей ProxyLogon, при этом полезной нагрузкой является программа-вымогатель DearCry.

После того, как мы сообщили об этой атаке, исследователь безопасности Microsoft Филип Миснер подтвердил, что DearCry, или то, что они называют DoejoCrypt, устанавливается при атаках, управляемых человеком, с использованием новых эксплойтов Microsoft Exchange.

Сегодня глава отдела кибер-расследований McAfee Джон Фоккер сообщил BleepingComputer, что они видят жертв в США, Люксембурге, Индонезии, Ирландии, Индии и Германии.

Хотя количество обнаружений все еще низкое, Фоккер заявляет, что количество обнаружений продолжает расти.

Поставщики антивирусных программ в настоящее время обнаруживают DearCry с помощью множества обычных средств обнаружения программ-вымогателей. Ниже мы перечислили более конкретные обнаружения:

Программы- вымогатели / Win.DoejoCrypt [AhnLab]
Win32 / Filecoder.DearCry.A [ESET]
Win32.Trojan-Ransom.DearCry.B [GDATA]
Ransom-DearCry [McAfee]
Выкуп: Win32 / DoejoCrypt.A [Microsoft]
Ransom.DearCry [возрастает]
Выкуп / W32.DearCry [TACHYON]
Ransom.Win32.DEARCRY [TrendMicro]
W32.Ransomware.Dearcry [Webroot]

Как программа-вымогатель DearCry шифрует компьютеры

Команда MalwareHunterTeam смогла найти три образца этого вымогателя на VirusTotal [1, 2, 3] с дополнительными хэшами, приведенными ниже, все из которых являются исполняемыми файлами, скомпилированными с помощью MingW…

При запуске программа-вымогатель DearCry создает службу Windows с именем «msupdate», которая запускается для шифрования. Эта служба Windows будет удалена позже, когда процесс шифрования будет завершен…

Гиллеспи сообщил BleepingComputer, что программа-вымогатель использует AES-256 для шифрования файлов и открытый ключ RSA-2048 для шифрования ключа AES. Кроме того, программа-вымогатель добавляет к надписи «ДОРОГОЕ!». строка в начало каждого зашифрованного файла.

После завершения шифрования компьютера программа-вымогатель создаст на рабочем столе Windows простую записку о выкупе с именем readme.txt. Эта записка с требованием выкупа содержит два адреса электронной почты злоумышленников и уникальный хэш, который, как утверждает Гиллеспи, является хешем MD4 открытого ключа RSA, встроенного во вредоносное ПО.

По крайней мере, за одну из жертв группа вымогателей потребовала выкуп в размере 16000 долларов.

К сожалению, программа-вымогатель не имеет недостатков, которые позволили бы жертвам бесплатно восстанавливать свои файлы.

Патч сейчас!

Согласно новым данным, предоставленным фирмой по кибербезопасности Palo Alto Networks с BleepingComputer, за последние три дня были исправлены десятки тысяч серверов Microsoft Exchange.

К сожалению, Palo Alto Networks заявляет, что все еще существует около 80 000 старых серверов, которые не могут напрямую применять последние обновления безопасности.

«Я никогда не видел такого высокого уровня исправлений безопасности для какой-либо системы, не говоря уже о такой широко распространенной, как Microsoft Exchange», - сказал Мэтт Крэнинг, технический директор Cortex в Palo Alto Networks. «Тем не менее, мы призываем организации, использующие все версии Exchange, предположить, что они были скомпрометированы, прежде чем они исправят свои системы, потому что мы знаем, что злоумышленники использовали эти уязвимости нулевого дня в дикой природе в течение как минимум двух месяцев, прежде чем Microsoft выпустила исправления 2 марта.»

Всем организациям настоятельно рекомендуется как можно скорее применить исправления и создать автономные резервные копии своих серверов Exchange…» ***(Lawrence Abrams. DearCry ransomware attacks Microsoft Exchange with ProxyLogon exploits // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/dearcry-ransomware-attacks-microsoft-exchange-with-proxylogon-exploits/). 11.03.2021).***

***

«Новая программа-вымогатель, известная как Sarbloh, шифрует ваши файлы и в то же время отправляет сообщение в поддержку протестов индийских фермеров.

В прошлом году правительство Индии приняло новый свод законов, названный «Законы о сельском хозяйстве Индии 2020 года»…

С ноября 2020 года тысячи индийских фермеров протестуют против этих законопроектов за пределами Нью-Дели.

Новый вымогатель Sarbloh поддерживает индийских фермеров

Как детализировано многочисленными охранные фирмы, в том числе Malwarebytes, Cyble и QuickHeal, новые вымогатели, известных как «Sarbloh» распространяются через вредоносные документы Word, которые содержат политическое послание в поддержке индийских фермеров.

Неизвестно, отправлен ли вредоносный документ Word через фишинговые электронные письма или другим способом, но при его открытии пользователям будет предложено «Включить содержимое», чтобы правильно просмотреть его содержимое.

Когда кнопка нажата, макросы документа Word загружают файл с именем putty.exe с помощью bitsadmin.exe в папку «Документы» и затем запускаются.

При запуске программа- вымогатель зашифрует файлы на компьютере, соответствующие определенным типам файлов, и добавит к имени файла расширение .sarbloh . Например, файл 1.jpg будет зашифрован и переименован в 1.jpg.sarbloh.

После того, как файлы на компьютере будут зашифрованы, будет создана записка о выкупе под названием README_SARBLOH.txt, содержащая сообщение в поддержку фермеров в Индии…

Похоже, что программа-вымогатель названа в честь «Сарбло Грант», книги Священных Писаний, связанных с сикхизмом.

По словам Майкла Гиллеспи, Sarbloh основан на программе-вымогателе с открытым исходным кодом, известной как KhalsaCrypt, которая, к сожалению, не имеет известных слабых мест.

Однако, в отличие от других программ-вымогателей, Sarbloh не удаляет копии теневых томов, поэтому возможно восстановление файлов через теневые тома». ***(Lawrence Abrams. New Sarbloh ransomware supports Indian farmers' protest // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-sarbloh-ransomware-supports-indian-farmers-protest/). 08.03.2021).***

***

«Предполагаемый участник программы-вымогателя GandCrab был арестован в Южной Корее за использование фишинговых писем для заражения жертв.

Операция вымогателя GandCrab началась в январе 2018 года, когда она быстро превратилась в империю вредоносных программ, угрожающую предприятиям по всему миру.

Работая как программа-вымогатель как услуга (RaaS), разработчики GandCrab объединились с аффилированными лицами в рамках партнерства по распределению доходов, при этом филиалы зарабатывают от 70 до 80% выкупа.

Операция прекратилась летом 2019 года, но многие исследователи безопасности считают, что основные разработчики создали группу вымогателей REvil.

В Южной Корее арестован подозреваемый аффилиат

Как впервые сообщил TheRecord, 20-летний мужчина был арестован 25 февраля полицией Южной Кореи после того, как международное расследование установило, что выплаты выкупа GandCrab осуществлялись подозреваемым.

Южнокорейские СМИ сообщают, что подозреваемый распространил 6 486 фишинговых писем. Эти письма якобы были отправлены полицией Южной Кореи, расследующей онлайн-клевету на адресата.

В электронные письма были вложены вложения, которые могли заразить жертву вымогателем GandCrab, зашифровать файлы и потребовать выкуп в биткойнах в размере 1300 долларов.

Хотя операторы GandCrab хвастались, что они получили выкуп в размере 2 миллиардов долларов, этот предполагаемый участник не разбогател от своей незаконной деятельности.

Полиция Южной Кореи заявляет, что подозреваемый заработал только 12 миллионов южнокорейских вон или примерно 10 500 долларов в рамках незаконной деятельности.

Полиция заявляет, что еще один подозреваемый, который поделился вымогателем GandCrab с арестованным, все еще находится на свободе.

В июле правоохранительные органы Беларуси также арестовали 31-летнего члена GandCrab, который участвовал в операции по вымогательству.

В этом году совместные операции правоохранительных органов уже имели большой успех в борьбе с бандами вымогателей. В прошлом месяце международные правоохранительные органы пресекли операции вымогателей Netwalker и Egregor». ***(Lawrence Abrams. GandCrab ransomware affiliate arrested for phishing attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-affiliate-arrested-for-phishing-attacks/). 09.03.2021).***

***

«Фирма по кибербезопасности Qualys, вероятно, является последней жертвой утечки данных после того, как уязвимость нулевого дня на их сервере Accellion FTA была использована для кражи размещенных файлов.

В декабре волна атак была направлена на приложение для обмена файлами Accellion FTA с использованием уязвимости нулевого дня, которая позволяла злоумышленникам красть файлы, хранящиеся на сервере.

С тех пор программа-вымогатель Clop вымогала у этих жертв, размещая украденные данные на их сайте утечки данных программ-вымогателей.

Поскольку устройства Accellion FTA представляют собой автономные серверы, предназначенные для того, чтобы находиться за пределами периметра безопасности сети и быть доступными для общественности, не сообщалось об атаках на эти устройства, приводящих к компрометации внутренних систем.

До сегодняшнего дня известные жертвы, вымогаемые Клопом, включают Transport for NSW, Singtel, Bombadier, специалиста по геоданным Fugro, юридическую фирму Jones Day, научно-техническую компанию Danaher и компанию технических услуг ABS Group.

Qualys последняя жертва, которую нужно вымогать

Вчера банда вымогателей Clop опубликовала скриншоты файлов, якобы принадлежащих фирме Qualys, занимающейся кибербезопасностью. Утечка данных включает заказы на покупку, счета-фактуры, налоговые документы и отчеты о сканировании.

Как сообщил Валерий Маркив из LegMagIT и подтвердил BleepingComputer, Qualys имеет устройство Accellion FTA, расположенное в их сети.

Устройство Accellion FTA было расположено по адресу fts-na.qualys.com, а IP-адрес, используемый сервером, назначен Qualys. Qualys с тех пор списала устройство FTA, а Shodan показывает, что последний раз оно было активным 18 февраля 2021 года.

Неизвестно, отправлял ли Клоп записки с требованием выкупа Qualys относительно атаки, но другие жертвы получали их в прошлом, согласно отчету Mandiant.

До сих пор неясно, выполняла ли банда вымогателей Clop атаки на устройства Accellion FTA или сотрудничает с другой группой, чтобы обмениваться файлами и публично вымогать у жертв.

В прошлом Clop отправлял журналистам, в том числе BleepingComputer, электронные письма о новых жертвах Accellion FTA, размещенных на их сайте.

BleepingComputer связалась с Qualys перед публикацией и ожидает официального заявления.

Qualys подтверждает нарушение Accellion FTA

В заявлении, опубликованном сегодня вечером, Qualys подтвердила, что их сервер Accellion FTA был взломан в декабре 2020 года и затронул ограниченное количество клиентов.

Поскольку сервер был развернут в их DMZ, которая отделена от их внутренней сети, среда продукта Qualys не была скомпрометирована.

«Сегодня появилась новая информация, связанная с ранее идентифицированным эксплойтом нулевого дня в стороннем решении Accellion FTA, которое Qualys развернула для передачи информации в рамках нашей системы поддержки клиентов».

«Qualys подтвердила, что не оказывает никакого влияния на производственные среды Qualys, кодовую базу или данные клиентов, размещенные на облачной платформе Qualys. Все платформы Qualys по-прежнему полностью функциональны, и никакого воздействия на работу не было».

«Qualys развернула сервер Accellion FTA в изолированной среде DMZ, полностью отделенной от систем, в которых размещены и поддерживаются продукты Qualys для передачи информации в рамках нашей системы поддержки клиентов», - сообщила Qualys в сегодняшнем сообщении об инциденте безопасности.

Qualys заявляет, что они отключили затронутые серверы Accellion FTA и переключились на альтернативные приложения для передачи файлов, связанных с поддержкой.

В настоящее время Qualys все еще расследует нарушение и наняла Mandiant для оказания им помощи». ***(Lawrence Abrams. Cybersecurity firm Qualys is the latest victim of Accellion hacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/cybersecurity-firm-qualys-is-the-latest-victim-of-accellion-hacks/). 03.03.2021).***

***

«Американский провайдер управляемых услуг CompuCom пострадал от атаки программы-вымогателя DarkSide, которая привела к отключению услуг и отключению клиентов от сети MSP для предотвращения распространения вредоносного ПО.

CompuCom - поставщик управляемых ИТ-услуг (MSP), который предоставляет компаниям удаленную поддержку, ремонт оборудования и программного обеспечения, а также другие технологические услуги. CompuCom является 100-процентной дочерней компанией ODP Corporation (Office Depot / Office Max), в которой работает около 8000 человек.

Некоторые из прошлых и существующих клиентов CompuCom включают хорошо известные имена, такие как Home Depot, Target, Citibank, Wells Fargo, Truist Bank и Lowe's.

Атака произошла на выходных

На выходных в CompuCom произошел сбой, из-за которого клиенты не могли получить доступ к клиентскому порталу компании, чтобы открыть заявки на устранение неполадок.

При посещении портала веб-сайт приветствовал клиентов общим сообщением об ошибке: «Произошла ошибка при обработке вашего запроса».

…CompuCom начала связываться с клиентами, чтобы предупредить их о том, что они были скомпрометированы вредоносным ПО вскоре после атаки. Однако клиентам не сообщили, какой тип атаки произошел и была ли это программа-вымогатель.

…CompuCom отключила их доступ к некоторым клиентам, чтобы предотвратить распространение вредоносного ПО. Другой клиент сообщил нам, что они отключились от VDI (инфраструктуры виртуальных рабочих столов) CompuCom, чтобы гарантировать, что их данные не пострадали от атаки.

Несколько человек также сказали BleepingComputer, что это была атака вымогателя, но мы не смогли подтвердить независимо, правда ли это.

После обращения в CompuCom по поводу атаки компания опубликовала заявление для BleepingComputer, в котором говорилось, что они пострадали от «инцидента с вредоносным ПО» и что нет никаких доказательств его распространения на системы клиентов.

Вы можете прочитать полный текст заявления CompuCom ниже: "Некоторые системы информационных технологий CompuCom пострадали от инцидента с вредоносным ПО, который влияет на некоторые услуги, которые мы предоставляем определенным клиентам. Наше расследование находится на ранней стадии и продолжается. В настоящее время у нас нет никаких указаний на то, что системы наших клиентов непосредственно пострадали от инцидента.

Как только нам стало известно о ситуации, мы немедленно приняли меры по ее сдерживанию и привлекли ведущих экспертов по кибербезопасности для начала расследования. Мы также общаемся с клиентами, чтобы сообщать им обновленную информацию о ситуации и предпринимаемых нами действиях.

Мы находимся в процессе восстановления обслуживания клиентов и внутренних операций как можно быстрее и безопаснее. Мы сожалеем о неудобствах, вызванных прерыванием работы, и ценим постоянную поддержку наших клиентов». - CompuCom

CompuCom подтверждает атаку программ-вымогателей в FAQ

Сегодня клиент CompuCom поделился «Часто задаваемыми вопросами клиентов относительно инцидента с вредоносным ПО», в котором содержится больше подробностей об атаке, чем компания поделилась в своем пресс-релизе.

Согласно часто задаваемым вопросам, компания CompuCom была взломана злоумышленниками, которые установили маяки Cobalt Strike на нескольких системах в своей среде.

Эти маяки позволяют удаленным злоумышленникам получить доступ к сети для кражи данных, распространения на другие машины и, в конечном итоге, развертывания программы-вымогателя, которую злоумышленники развернули 28 февраля.

«На основании анализа, проведенного нашим экспертом на сегодняшний день, мы понимаем, что злоумышленник развернул постоянный бэкдор Cobalt Strike на нескольких системах в среде и получил учетные данные администратора. Эти учетные данные были затем использованы для развертывания программы-вымогателя Darkside», - говорится в часто задаваемых вопросах CompuCom.

Cobalt Strike все чаще распространяется с помощью различных троянов, устанавливаемых с помощью фишинговых кампаний. К этим троянам относятся BazarLoader, TrickBot, ZLoader и QBot.

Теперь, когда подтверждено, что за атакой стоит программа-вымогатель DarkSide, вполне вероятно, что злоумышленники собирали незашифрованные файлы перед шифрованием устройств.

Если данные были украдены, а выкуп не выплачен, мы, вероятно, увидим, что эти данные будут опубликованы на их сайте утечки данных программ-вымогателей в ближайшие несколько недель…». ***(Lawrence Abrams. CompuCom MSP hit by DarkSide ransomware cyberattack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/compucom-msp-hit-by-darkside-ransomware-cyberattack/). 04.03.2021).***

***

«Член киберпреступного сообщества обнаружил и опубликовал уязвимость в вымогательском ПО LockBit, которую можно было бы использовать для создания бесплатного декриптора.

LockBit распространяется по бизнес-модели "вымогательское ПО как услуга" (ransomware-as-a-service, RaaS) с января 2020 года. Разработчики вредоноса сдают его в аренду своим клиентам или так называемым "партнерам". Эти "партнеры" получают доступ к корпоративным сетям и развертывают в них вымогательское ПО, которое шифрует файлы и требует выкуп за их восстановление.

В отображающейся на рабочем столе записке с требованием выкупа жертвам LockBit предлагается получить доступ к web-порталу в даркнете, где они могут договориться с вымогателями об оплате. На этом портале также доступна одноразовая бесплатная функция дешифрования, доказывающая жертвам, что у хакеров есть рабочая копия ключа для расшифровки файлов.

В среду, 17 марта, на киберпреступном форуме были опубликованы подробности об уязвимости в одноразовой функции дешифрования LockBit, с помощью которой эксперты могли бы создать инструмент для восстановления файлов без уплаты выкупа. Публикация была сделана предположительно русскоязычным киберпреступником Bassterlord, который ранее был "партнером" группировок LockBit, REvil, Avaddon и RansomExx.

Теперь, когда об уязвимости стало известно широкой общественности, разработчики LockBit могут ее исправить, и шанс создать инструмент для бесплатного восстановления файлов будет упущен». ***(Хакер опубликовал уязвимость в вымогательском ПО LockBit // SecurityLab.ru (https://www.securitylab.ru/news/517573.php). 18.03.2021).***

***

«Group-IB ппредставила новый отчет «Программы-вымогатели 2020-2021» — масштабное исследование одной из самых актуальных киберугроз в период пандемии COVID-19. В прошлом году количество атак шифровальщиков выросло более чем на 150% по сравнению с предыдущим годом.

Среднее время простоя атакованной компании —18 суток, а сумма выкупа увеличилась почти вдвое — до $170 000. Основными целями хакеров стали корпоративные сети крупных компаний из Северной Америки, Европы, Латинской Америки, Азиатско-Тихоокеанского региона. Первые атаки эксперты фиксировали и в России: прогнозируется, что в 2021 году волна шифровальщиков затронет российский бизнес и выйдет в СНГ.

«Золотая лихорадка» 2020 года

Программы-шифровальщики стали киберугрозой №1 как для бизнеса, так и для государственных органов: число успешных атак в прошлом году выросло более чем на 150% к 2019 году, а средний размер суммы выкупа увеличился более чем в два раза и составил в 2020 году $170 000. Самыми жадными вымогателями оказались Maze, DoppelPaymer и RagnarLocker. Сумма выкупа, который они требовали от жертвы, составляла в среднем от $1 000 000 до $2 000 000.

В зоне риска оказались крупные корпоративные сети — целенаправленные атаки вымогателей (The Big Game Hunting) парализовали в 2020 году работу таких гигантов как Garmin, Canon, Campari, Capcom и Foxconn. Простой бизнеса от одной атаки, в среднем, составлял в среднем 18 дней. Большинство атак, проанализированных Group-IB, произошли в Северной Америке и Европе, где расположено большинство компаний из списка Fortune 500, а также в Латинской Америке и Азиатско-Тихоокеанском регионе.

В России, несмотря на негласное правило у киберпреступников «не работать по РУ», действовала русскоязычная преступная группа OldGremlin — впервые Group-IB рассказала о ней в отчете в сентябре прошлого года. Начиная с весны 2020 года OldGremlin провела не менее 9 кампаний и атаковала исключительно российский бизнес — банки, промышленные предприятия, медицинские организации и разработчиков софта. В августе 2020 года жертвой OldGremlin стала крупная компания с сетью региональных филиалов— за расшифровку с нее потребовали выкуп в $50 000.

«За пандемию программы-вымогатели стали главной киберугрозой для всего мира, в том числе для России, — говорит Олег Скулкин, ведущий специалист Лаборатории компьютерной криминалистики Group-IB. — В прошлом году мы видели многочисленные атаки OldGremline на российские предприятия, IT-компании и финансовые учреждения. В этом году эксперты уже наблюдают активность с традиционными группами типа RTM, также переключившихся на на использование шифровальщиков».

Mortal Kombat: очень организованная преступность

Одной из основных движущих сил феноменального роста программ-вымогателей стала модель Ransomware-as-a-Service («Вымогательство как услуга»). Ее смысл заключается в том, что разработчики продают или сдают в аренду свои вредоносные программы партнерам для использования в их атаках с целью компрометации сети, заражения и развертывания вымогателей. Вся полученная в

виде выкупа прибыль затем распределяется между операторами и партнерами программы. Команда Group-IB DFIR отмечает, что 64% всех атак вымогателей, проанализированных в 2020 году, были связаны с операторами, использующих модель RaaS.

Еще одна тенденция 2020 года — коллаборация между разными преступными группами. Group-IB Threat Intelligence & Attribution system зафиксировала в прошлом году появление в андеграунде 15 новых публичных партнерских программ-вымогателей. Действующие преступные группы, использующие вредоносные программы Trickbot, Qakbot и Dridex, все чаще помогали операторам программ-вымогателей получать первоначальный доступ к корпоративным сетям.

Главным вектором атак для большинства банд вымогателей оказались публичные RDP-серверы (52%). На втором месте —фишинг (29%), затем эксплуатация общедоступных приложений (17%).

Прежде чем зашифровать данные, операторы вымогателей проводили в среднем 13 дней в скомпрометированной сети, стараясь предварительно найти и удалить все доступные резервные копии, чтобы жертва не могла восстановить зашифрованные файлы. Еще одним фактором успеха, позволившим бандам получать выкуп, стало предварительное хищение критически важных данных — документов, отчетов, чтобы использовать их в качестве рычага для давления на жертву — моду на подобный «двойной удар» задала печально известная группа Maze.

Учитывая, что большинство атак шифровальщиков управляются человеком — «вручную», специалистам по информационной безопасности критически важно понимать, какие тактики, техники и процедуры (TTP) используют злоумышленники. Полный технический анализ TTPs атакующих, сопоставленных в соответствии с MITRE ATT&CK®,, публичной базой знаний, в которой собраны тактики и техники целевых атак, .а также рекомендации по поиску и обнаружению угроз, собранные командой Group-IB Digital Forensics and Incident Response (DFIR), уже сейчас доступны в новом отчете «Программы-вымогатели 2020-2021 гг». ***(Количество атак шифровальщиков выросло за год более чем на 150% // SecurityLab.ru (https://www.securitylab.ru/news/517140.php). 04.03.2021).***

***

«Программы-шифровальщики стали киберугрозой №1 как для бизнеса, так и для государственных органов: число успешных атак в прошлом году выросло более чем на 150% к 2019 году, а средний размер суммы выкупа увеличился более чем в два раза и составил в 2020 году $170 000.

Самыми жадными вымогателями оказались Maze, DoppelPaymer и RagnarLocker. Сумма выкупа, который они требовали от жертвы, составляла в среднем от $1 000 000 до $2 000 000. Такие данные опубликованы в отчете «Программы-вымогатели 2020-2021», подготовленном компанией Group-IB.

В зоне риска оказались крупные корпоративные сети — целенаправленные атаки вымогателей (The Big Game Hunting) парализовали в 2020 году работу таких гигантов как Garmin, Canon, Campari, Capcom и Foxconn. Простой бизнеса от одной

атаки, в среднем, составлял в среднем 18 дней. Большинство атак, проанализированных Group-IB, произошли в Северной Америке и Европе, где расположено большинство компаний из списка Fortune 500, а также в Латинской Америке и Азиатско-Тихоокеанском регионе.

В России, несмотря на негласное правило у киберпреступников «не работать по РУ», действовала русскоязычная преступная группа OldGremlin — впервые Group-IB рассказала о ней в отчете в сентябре прошлого года. Начиная с весны 2020 года OldGremlin провела не менее 9 кампаний и атаковала исключительно российский бизнес — банки, промышленные предприятия, медицинские организации и разработчиков софта. В августе 2020 года жертвой OldGremlin стала крупная компания с сетью региональных филиалов— за расшифровку с нее потребовали выкуп в $50 000.

«За пандемию программы-вымогатели стали главной киберугрозой для всего мира, в том числе для России, — говорит Олег Скулкин, ведущий специалист Лаборатории компьютерной криминалистики Group-IB. — В прошлом году мы видели многочисленные атаки OldGremline на российские предприятия, IT-компании и финансовые учреждения. В этом году эксперты уже наблюдают активность с традиционными группами типа RTM, также переключившихся на на использование шифровальщиков».

Одной из основных движущих сил феноменального роста программ-вымогателей стала модель Ransomware-as-a-Service («Вымогательство как услуга»). Ее смысл заключается в том, что разработчики продают или сдают в аренду свои вредоносные программы партнерам для использования в их атаках с целью компрометации сети, заражения и развертывания вымогателей. Вся полученная в виде выкупа прибыль затем распределяется между операторами и партнерами программы. Команда Group-IB DFIR отмечает, что 64% всех атак вымогателей, проанализированных в 2020 году, были связаны с операторами, использующих модель RaaS.

Еще одна тенденция 2020 года — коллаборация между разными преступными группами. Group-IB Threat Intelligence & Attribution system зафиксировала в прошлом году появление в андеграунде 15 новых публичных партнерских программ-вымогателей. Действующие преступные группы, использующие вредоносные программы Trickbot, Qakbot и Dridex, все чаще помогали операторам программ-вымогателей получать первоначальный доступ к корпоративным сетям.

Главным вектором атак для большинства банд вымогателей оказались публичные RDP-серверы (52%). На втором месте —фишинг (29%), затем эксплуатация общедоступных приложений (17%).

Прежде чем зашифровать данные, операторы вымогателей проводили в среднем 13 дней в скомпрометированной сети, стараясь предварительно найти и удалить все доступные резервные копии, чтобы жертва не могла восстановить зашифрованные файлы. Еще одним фактором успеха, позволившим бандам получать выкуп, стало предварительное хищение критически важных данных — документов, отчетов, чтобы использовать их в качестве рычага для давления на жертву — моду на подобный «двойной удар» задала печально известная группа

Maze…». ***(Аналитики назвали киберугрозу №1 // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5722744-Analitiki-nazvali-kiberugrozu.html). 04.03.2021).***

***

«Организация по регулированию инвестиционной индустрии Канады («IIROC») опубликовала Уведомление о кибербезопасности в отношении программ-вымогателей («Уведомление»), в котором отмечается недавний всплеск атак программ-вымогателей на фирмы IIROC и дается руководство о том, как фирмам IIROC следует предотвращать, обнаруживать и реагировать для защиты от атак программ-вымогателей и восстановления после них.

Программы-вымогатели стали самым распространенным киберпреступлением. В то время как программы-вымогатели по своей сути представляют собой атаку на компьютерные системы, основанную на вредоносном ПО, которая приводит к шифрованию данных и требованию выкупа, в настоящее время оно все чаще использует модель «двойного вымогательства», когда конфиденциальные данные (личная информация и / или конфиденциальные бизнес-данные) являются извлечены из этих систем, с угрозой опубликовать их, если не будет уплачен выкуп.

Уведомление является последней разработкой в постоянных усилиях IIROC по повышению готовности фирм к кибербезопасности и следует за рядом связанных уведомлений, включая Уведомление о кибербезопасности IIROC об обязательном сообщении об инцидентах (которое мы обсуждали в нашем предыдущем сообщении в блоге).

Каковы последствия Уведомления о кибербезопасности IIROC для программ-вымогателей?

Фирмы-члены IIROC должны осознавать повышенный риск атак программ-вымогателей и должны внедрять комплексные меры по предотвращению, обнаружению, смягчению, реагированию и восстановлению после таких атак. Уведомление представлено как набор рекомендаций относительно того, что фирмы IIROC должны делать как минимум для снижения риска, но рекомендации не являются исчерпывающими.

Какие стратегии защиты, идентификации и обнаружения рекомендует IIROC?

IIROC определяет ключевые векторы угроз для программ-вымогателей, в том числе:

Фишинговые атаки, т. Е. Компрометация системы посредством нажатия сотрудниками вредоносных ссылок или вложений;

«Попутные загрузки», т. Е. Лица, посещающие взломанные веб-сайты или нажимающие на вредоносные рекламные объявления на законных веб-сайтах;

Украденные учетные данные стали доступными в результате повторного использования сотрудниками взломанных учетных данных в рабочем контексте; и

Вступление в уязвимые сети или серверы методом грубой силы.

Чтобы предотвратить развертывание программ-вымогателей, IIROC рекомендует компаниям установить комплексные меры контроля, которые должны включать:

Контроль, политики и процедуры на уровне компании, обеспечивающие быстрое устранение аномального поведения и быстрое расследование предполагаемых атак.

Средства управления резервным копированием информации для обеспечения резервного копирования всех систем и данных (с частым резервным копированием важной информации), а также того, что все резервные копии проверяются на целостность и хранятся отдельно от производственных сетей.

Технологические средства управления для защиты устройств и сетей, включая строгие средства управления доступом, регулярные обновления системы, инструменты веб-фильтрации, ограничения доступа к удаленному рабочему столу, возможности защиты от вредоносных программ и вирусов в ключевых точках среды (включая «песочницу» для безопасного тестирования вредоносных вложений), а также платформу управления информацией и событиями безопасности (SIEM) для агрегирования данных о событиях и безопасности для помощи в реагировании и восстановлении.

Обучение сотрудников, подрядчиков и консультантов с целью поощрения бдительности при переходе по ссылкам, в том числе посредством частых тренингов и тестов на осведомленность о фишинге, а также регулярных напоминаний о протоколах реагирования фирмы и важности уведомления ИТ при обнаружении необычной активности.

Мониторинг аномального поведения для обнаружения и смягчения атак, в том числе путем реализации функции непрерывного мониторинга безопасности («CSM») и решения для обнаружения угроз и реагирования на конечные точки («EDTR»), а также с помощью других инструментов для отслеживания вредоносных адресов и сетевого трафика. активность и ненормальная активность входа в систему (включая необычные боковые движения по сети).

В рамках контроля на уровне фирмы IIROC также рекомендует учитывать, какой тип и размер страхования кибербезопасности подходят с учетом уровней риска фирмы. Важность получения отдельных кибер-конкретные страховые полисы недавно было подчеркнуто в решении от Онтарио Апелляционного суда, в котором суд суженной наличие страхового покрытия по вопросам кибер при традиционных страховых полисов (см наше недавнее сообщение в блоге для более подробной информации о дело, Служба поддержки семьи и детей Ланарка, Лидса и Гренвилля против Кооператора General Insurance Company, 2021 ONCA 0159).

Какие стратегии восстановления и реагирования рекомендует IIROC?

IIROC рекомендует фирмам внедрить средства управления, чтобы помочь с восстановлением и реагированием в случае атаки программы-вымогателя, что должно потребовать от фирмы:

Немедленно изолируйте зараженное устройство, чтобы ограничить масштаб атаки, в том числе с помощью мер защиты сети, таких как обновления, приостановка учетной записи и требование новых учетных данных для входа.

Определите, доступна ли для каких-либо данных пригодная для восстановления чистая резервная копия, и если да, убедитесь, что резервная копия не содержит вредоносных программ и что восстановление данных не препятствует тщательному судебно-медицинскому расследованию, и проконсультируйтесь с юрисконсультом по поводу любого решения платить или не платить выкуп.

Изучите инцидент, чтобы оценить масштаб атаки, в том числе путем привлечения внешней группы судебно-медицинских экспертов для определения первопричины и определения того, произошло ли нарушение данных, которое затронуло личную или конфиденциальную информацию (и если да, следуйте протоколам реагирования на инциденты, включая любые применимые требования к уведомлению). (Кроме того, может быть целесообразно проконсультироваться с тренером по нарушению правил до того, как привлекать эту группу судебно-медицинских экспертов, чтобы оценить правовую стратегию и лучше понять роль адвоката-клиента и судебной привилегии в контексте реагирования на нарушение).

Сообщите об инциденте соответствующим органам, включая уполномоченных по вопросам конфиденциальности, регулирующих органов и правоохранительных органов, и предоставьте всю необходимую информацию менеджеру по соблюдению требований финансового и операционного законодательства IIROC, если инцидент подпадает под действие правила IIROC 3100 (B.1.1) Отчетность о кибербезопасности.

Интересно, что IIROC не занимается сложным (и юридически сложным) вопросом оценки того, следует ли платить выкуп для восстановления данных или предотвращения публикации личной информации. Такое решение связано со сложными и быстро развивающимися юридическими и практическими соображениями, которые следует оценивать в каждом конкретном случае с помощью опытных практиков». ***(Gregory Corosky, Daniel G.C. Glover, Michael Scherman. IIROC Publishes Notice Regarding Ransomware Attacks // McCarthy Tétrault (https://www.mccarthy.ca/en/insights/blogs/techlex/iiroc-publishes-notice-regarding-ransomware-attacks#page=1). 23.03.2021).***

***

«Исследователи из CrowdStrike, Accenture и Awake Security проанализировали некоторые атаки с использованием вымогателя Hades и опубликовали информацию как о самом вредоносном ПО, так и о тактике, методах и процедурах (TTP), используемых его операторами.

Первоначально наблюдавшаяся в декабре 2020 года программа-вымогатель с одноименным названием Hades (другое семейство вредоносных программ от вымогателя Hades Locker, появившегося в 2016 году) использует тактику двойного вымогательства, извлекая данные о жертвах и угрожая их публичной утечкой, если выкуп не будет оплачен.

Злоумышленник, по всей видимости, в основном сосредоточен на предприятиях, причем некоторые жертвы - это многонациональные организации с годовым доходом более 1 миллиарда долларов. Атаки в основном затронули Канаду, Германию, Люксембург, Мексику и США.

Операторы программы-вымогателя Hades нацелены только на несколько отраслей, включая транспорт и логистику, производство потребительских товаров, а также производство и распространение. Известными жертвами являются поставщик логистических услуг и организации, участвующие в цепочке поставок автомобилей и производстве изоляционных материалов. По крайней мере, трое из жертв - американские компании с годовым доходом более 1 миллиарда долларов, отмечает Accenture.

В записке о выкупе, брошенной на скомпрометированные машины, каждая жертва направляется на уникальный веб-сайт Tor - на сегодняшний день было идентифицировано шесть таких сайтов, что позволяет предположить, что Аид сделал не менее шести жертв. На этом веб-сайте жертве предлагается связаться со злоумышленниками с помощью одноранговой мессенджера Tox.

Операторы программ-вымогателей требуют от своих жертв выплат в размере от 5 до 10 миллионов долларов. Интересно, что, несмотря на относительно небольшое количество жертв и большие требования к оплате, злоумышленники, похоже, медленно реагируют на запросы инструкций по выплате выкупа.

Помимо шифрования файлов на машинах жертвы, операторы программы-вымогателя Hades также извлекают данные, которые считаются представляющими интерес, и вынуждают жертву заплатить выкуп, угрожая опубликовать украденные данные.

Однако в тех немногих случаях, когда злоумышленники реализовали свою угрозу, утечка оказала небольшое влияние на жертву, несмотря на то, что во время атаки были извлечены гораздо более ценные данные.

«Возникает вопрос: с какой целью были украдены драгоценности короны, но не были раскрыты менее важные части информации? Неужели они воздерживались от публичного обмена наиболее ценными данными, потому что у них были альтернативные способы монетизации служебных секретов?» Заметки для пробуждения.

Типичная атака программы-вымогателя Hades включает использование законных учетных данных для подключения к системам с выходом в Интернет через протокол удаленного рабочего стола (RDP) или виртуальную частную сеть (VPN) с последующим развертыванием имплантатов Cobalt Strike и Empire для обеспечения устойчивости.

Злоумышленники также используют различные сценарии для проведения разведки, сбора учетных данных для повышения привилегий, когда это необходимо, а также для выявления и взлома дополнительных систем в сети.

В некоторых случаях злоумышленник скомпилировал двоичный файл вымогателя одновременно с удалением данных из среды жертвы. Считается, что злоумышленники использовали в своих атаках подход «руки на клавиатуре».

Однако пока неясно, кто именно мог управлять Аидом. Хотя Accenture еще не установила атрибуцию, Awake установила некоторые связи с другими злоумышленниками, включая Hafnium, китайскую хакерскую группу, участвовавшую в недавно раскрытых взломах Exchange Server.

CrowdStrike, с другой стороны, считает, что Hades - это работа печально известной банды Evil Corp, российского злоумышленника, известного

использованием трояна Dridex, программ-вымогателей Locky и множества других семейств вредоносных программ. Hades, по данным службы безопасности, демонстрирует множество сходств кода с WastedLocker, вымогателем, приписываемым Evil Corp в прошлом году.

«Hades - это просто 64-битный скомпилированный вариант WastedLocker с дополнительным запутыванием кода и незначительными изменениями функций. […] Программа-вымогатель Hades разделяет большую часть своих функций с WastedLocker; статическая конфигурация, основанная на ISFB, многоэтапный процесс сохранения / установки, перечисление файлов / каталогов и функции шифрования практически не изменились», - отмечает CrowdStrike.

Кроме того, охранная фирма заявляет, что Hades также отмечает изменения в ТТП, используемых Evil Corp (также известными как TA505 и INDRIK SPIDER), что может быть реакцией на объявление Управления по контролю за иностранными активами Министерства финансов США (OFAC) санкций против банда и Министерство юстиции предъявили обвинения двум членам группы…». ***(Ionut Arghire. 'Hades' Ransomware Hits Big Firms, but Operators Slow to Respond to Victims // Wired Business Media (https://www.securityweek.com/hades-ransomware-hits-big-firms-operators-slow-respond-victims). 29.03.2021).***

***

«Атака программы-вымогателя заразила ИТ-системы в школах по всему Лондону, в результате чего десятки тысяч учеников остались без доступа к электронной почте и выданным школам устройствам.

Федерация Харриса, которая управляет 50 начальными и средними школами в Лондоне и Эссексе, стала жертвой атаки с использованием программ-вымогателей в субботу, 27 марта - всего через несколько дней после того, как Национальный центр кибербезопасности (NCSC) объявил о предупреждении школ, колледжей и университетов о заражении. «растущая угроза» киберпреступников, нацеленных на образование с помощью программ-вымогателей.

Федерация Харриса выявила, что киберпреступники получали доступ к ИТ-системам и зашифровывали данные с помощью скрытой формы программы-вымогателя.

В заявлении Федерации Харриса говорится, что атака программ-вымогателей окажет «значительное влияние» и что в качестве меры предосторожности система электронной почты была отключена. Школьные телефонные службы, которые также работают через Интернет, также были отключены, за исключением некоторых «очень ограниченных» услуг коммутации.

Учащиеся, которым школы выдали устройства, в настоящее время не могут ими пользоваться, поскольку в качестве меры предосторожности они отключены.

Школа привлекла «специализированную фирму консультантов по кибертехнологиям для расследования точных деталей атаки программ-вымогателей, а также работает с Национальным агентством по борьбе с преступностью (NCA) и NCSC. намечено в марте", - сказано в сообщении.

Федерация Харриса не детализировала точный характер информации, которая была получена и зашифрована киберпреступниками, но заявляет, что

признает, что семьи школьников будут иметь «индивидуальные опасения по поводу данных».

ZDNet попытался связаться с Федерацией Харриса для получения дополнительной информации об атаке программы-вымогателя, но на момент публикации ответа не получил.

Федерация Харриса - последняя в череде школ, колледжей и университетов, пострадавших от атак программ-вымогателей…». ***(Danny Palmer. A highly sophisticated ransomware attack leaves 36,000 students without email // ZDNet (https://www.zdnet.com/article/a-highly-sophisticated-ransomware-attack-leaves-36000-students-without-email/). 30.03.2021).***

***

«Sierra Wireless, международный производитель устройств Интернета вещей, возобновил производство после атаки программы-вымогателя.

Канадская компания стала жертвой атаки программ-вымогателей на ее ИТ-системы 20 марта, нарушив внутренние операции и производственные мощности.

Но теперь Sierra Wireless восстановила производство на своих производственных площадках и работает над восстановлением внутренних сетей.

Компания работала с юридической фирмой по кибербезопасности Blake, Cassels and Graydon LLP и следователями по кибербезопасности из KMPG в ответ на атаку программ- вымогателей и проанализировала то, что произошло.

«Безопасность является главным приоритетом, и Sierra Wireless обязуется принимать все необходимые меры для обеспечения высочайшей целостности всех наших систем», - сказал Сэм Кокрейн, финансовый директор Sierra Wireless.

«Я горжусь усилиями нашей ИТ-команды и внешних консультантов, поскольку они смягчили атаку и добились реального прогресса в налаживании операций», - добавил Кокрейн.

Воздействие атаки ограничивалось внутренними системами Sierra Wireless, а продукты, предназначенные для клиентов, не были затронуты программами-вымогателями, поскольку ИТ-системы для внутренних операций и ИТ-системы для операций клиентов разделены.

«На данном этапе расследования атаки с использованием программ-вымогателей компания не ожидает, что в результате атаки потребуются какие-либо исправления безопасности для продуктов или обновления прошивки или программного обеспечения», - говорится в заявлении компании.

Пока неясно, когда будут восстановлены оставшиеся системы, пострадавшие от атаки вымогателя. На момент написания Sierra Wireless не раскрыла, какая форма вымогателя зашифровала сеть и как организация стала жертвой кибератаки…». ***(Danny Palmer. Sierra Wireless partially restores network following ransomware attack // ZDNet (https://www.zdnet.com/article/sierra-wireless-partially-restores-network-following-ransomware-attack/). 26.03.2021).***

***

«Royal Dutch Shell - последняя корпорация, зараженная вымогателем Clop. Преступники, стоящие за вредоносным ПО, перекачали внутренние

документы нефтяного гиганта и публично слили некоторые данные - в частности, подборку сканированных паспортов рабочих и виз, - чтобы заставить корпорацию заплатить выкуп.

Ранее в этом месяце нефтяной гигант признал, что его системы были скомпрометированы, написав в заявлении, что «неавторизованная сторона получила доступ к различным файлам в течение ограниченного периода времени».

Он попытался преуменьшить влияние, отметив, что «нет никаких доказательств какого-либо воздействия на основные ИТ-системы Shell», а доступ к серверу был «изолирован от остальной цифровой инфраструктуры Shell». Но он признал, что мошенники, вероятно, захватили «некоторые личные данные и ... данные от компаний Shell и некоторых из их заинтересованных сторон».

Чтобы побудить Shell заплатить выкуп, чтобы не только расшифровать любые файлы, зашифрованные Clop, но и предотвратить их утечку ворами, мы отметили в понедельник, что банда загрузила на свой скрытый Tor веб-сайт подборку документов, в том числе сканы предполагаемых Shell. визы сотрудников в США, а также страницу паспорта и файлы из американских и венгерских офисов. Идея состоит в том, что если выкуп, обычно в криптовалюте, выплачивается, данные больше не сбрасываются в онлайн.

Мы не делимся ссылкой на материал по понятным причинам.

Тактика кражи и давления - это лишь последнее в череде преступлений банды Clop, которая в первую очередь преследовала организации, развернувшие уязвимые версии устаревшего устройства передачи файлов Accellion, используя программное обеспечение для кражи внутренней информации. И поэтому неудивительно видеть заметку нефтяного гиганта: «Shell пострадала от инцидента с безопасностью данных, связанного с устройством передачи файлов Accellion. Shell использует это устройство для безопасной передачи больших файлов данных».

Представитель Shell не был доступен для немедленных комментариев по вышеупомянутым утечкам.

Ранее в этом месяце на скрытом сайте вымогателей также появились файлы информационной службы Qualys, включая заказы на поставку, результаты сканирования устройств и расценки. И это далеко не один.

Среди других жертв - канадская аэрокосмическая компания Bombardier, обнаружившая утечку информации о радаре военного класса, лондонское рекламное агентство The7stars и немецкий гигант Software AG.

И чтобы усилить давление, банда Clop теперь отправляет электронные письма клиентам своих жертв, предупреждая, что данные были украдены и будут утечкой, если выкуп не будет уплачен, в попытке заставить упомянутых клиентов потребовать выплаты вымогателям…». ***(Kieren McCarthy. After oil giant Shell hit by Clop ransomware, workers' visas dumped online as part of extortion attempt // The Register (https://www.theregister.com/2021/03/29/shell_clop_ransomware_leaks/). 29.03.2021).***

***

«После недавнего объявления о завершении операции администратор программы-вымогателя Ziggy теперь заявляет, что они также вернут деньги.

Похоже, что это запланированный шаг, поскольку администратор поделился «хорошими новостями» чуть больше недели назад, но не сообщил подробностей.

Завершение работы с последующим возвращением денег

Программа-вымогатель Ziggy закрылась в начале февраля. В коротком объявлении администратор операции сказал, что они «опечалены» тем, что они сделали, и что они «решили опубликовать все ключи дешифрования».

На следующий день, 7 февраля, они предложили SQL-файл с 922 ключами дешифрования, который жертвы могли использовать для разблокировки своих файлов.

Администратор также предоставил инструмент дешифрования, чтобы упростить процесс, вместе с исходным кодом для дешифратора, для работы которого не требуется подключение к Интернету.

19 марта администратор программы-вымогателя Ziggy заявил, что также хочет вернуть деньги жертвам, которые заплатили выкуп. Сегодня после недельного молчания админ сообщил, что готовы отменить платежи.

Жертвы должны связаться с администратором по указанному адресу электронной почты (ziggyransomware@secmail.pro) с подтверждением их оплаты в биткойнах и идентификатором компьютера, и деньги будут возвращены в биткойн-кошелек жертвы примерно через две недели.

Возврат выкупа и получение прибыли

Жертвы программ-вымогателей получают записку о выкупе с инструкциями о том, как связаться с киберпреступниками, чтобы договориться о платеже. Обычно платеж согласовывается в фиате, но оплачивается в биткойнах.

В разговоре с BleepingComputer администратор программы-вымогателя Ziggy сказал, что возмещение будет в биткойнах по стоимости в день платежа.

Цена биткойна росла в течение последних трех месяцев, и на момент написания его цена близка к 55000 долларов.

В день, когда ключи расшифровки вымогателей Ziggy стали общедоступными, цена биткойнов составляла около 39000 долларов. За пять дней до того, как администратор объявил, что они вернут деньги, биткойн поднялся выше 61000 долларов. Учитывая разницу в цене, администратор получает прибыль по текущей цене биткойнов.

Администратор программы-вымогателя Ziggy сказал BleepingComputer, что они живут в «стране третьего мира» и что их мотивация для создания шкафчика была финансовой. Они подтвердили нам, что недавние действия вызваны опасением, что правоохранительные органы их поймают. Недавняя активность, которая нарушила гораздо более крупные операции, такие как программы-вымогатели Emotet и Netwalker, вероятно, во многом повлияла на это решение.

Администратор также утверждает, что им пришлось продать свой дом, чтобы иметь возможность возместить жертвам программы-вымогателя Ziggy, и что они планируют перейти на другую сторону и стать охотником на вымогателей после возврата денег». ***(Ionut Ilascu. Ransomware admin is refunding victims their ransom payments // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ransomware-admin-is-refunding-victims-their-ransom-payments/). 28.03.2021).***

***

«Предупреждение Федерального бюро расследований США о программе-вымогателе Mamba обнаруживает слабое место в процессе шифрования, которое может помочь целевым организациям оправиться от атаки без выплаты выкупа.

ФБР предупреждает, что атаки программы-вымогателя Mamba были направлены на организации в государственном и частном секторе, включая местные органы власти, транспортные агентства, юридические услуги, технологические услуги, промышленные, коммерческие, производственные и строительные предприятия.

Гонка за ключом шифрования

Программа-вымогатель Mamba (также известная как HDDCryptor) полагается на программное решение с открытым исходным кодом DiskCryptor для шифрования компьютеров-жертв в фоновом режиме с помощью ключа, определенного злоумышленником

ФБР объясняет, что для установки DiskCryptor требуется перезагрузка системы для добавления необходимых драйверов, что происходит с Mamba примерно через две минуты после развертывания программы.

Агентство также отмечает, что ключ шифрования и переменная времени выключения хранятся в конфигурации DiskCryptor, в текстовом файле с именем myConf.txt.

Второй перезапуск системы происходит после завершения процесса шифрования, примерно через два часа, и записка о выкупе становится доступной.

Поскольку в отношении ключа шифрования нет защиты, поскольку он сохраняется в виде открытого текста, ФБР заявляет, что этот двухчасовой перерыв - возможность для организаций, пострадавших от вымогателя Mamba, восстановить его.

Операция вымогателя Mamba начала увеличивать свою активность с появлением нового варианта, обнаруженного во второй половине 2019 года. Несмотря на отсутствие партнерской программы, она была одной из основных угроз.

Согласно отчету Coveware, в первом квартале прошлого года Mamba входила в пятерку основных угроз вымогателей во главе с REvil и Ryuk. Ситуация изменилась в четвертом квартале 2020 года, хотя по-прежнему представляет собой значительный риск.

Одна из особенностей программы-вымогателя Mamba заключается в том, что она перезаписывает основную загрузочную запись (MBR) диска, предотвращая доступ к зашифрованным файлам на диске. Это затрудняет отслеживание количества атак, поскольку файлы нельзя анализировать с помощью автоматических сервисов, таких как ID-Ransomware...» ***(Ionut Ilascu. FBI exposes weakness in Mamba ransomware, DiskCryptor // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fbi-exposes-weakness-in-mamba-ransomware-diskcryptor/). 26.03.2021).***

***

«Американский провайдер управляемых услуг CompuCom ожидает убытков в размере более 20 миллионов долларов после атаки программы-вымогателя DarkSide в этом месяце, в результате которой было разрушено большинство его систем.

CompuCom - поставщик управляемых ИТ-услуг (MSP) и дочерняя компания, находящаяся в полной собственности корпорации ODP (Office Depot / Office Max).

Штат MSP, насчитывающий более 8000 сотрудников, обеспечивает ремонт оборудования и программного обеспечения, удаленную поддержку и другие технические услуги для крупных компаний, включая Citibank, Home Depot, Wells Fargo, Target, Trust Bank и Lowe's.

Некоторые расходы покрывает киберстрахование

«По оценкам компании потеря доходов составит от $ 5,0 млн и 8,0 млн $ в результате инцидента (в первую очередь из - за CompuCom нуждаются временно приостановить определенные услуги определенным клиентам),» CompuCom материнская компания, корпорация ODP, показали в пятницу.

«Кроме того, Компания ожидает понести расходы в размере до 20 миллионов долларов, из которых, как предполагает Компания, примерно 10 миллионов долларов будут начислены в течение первого квартала 2021 года».

Расходы в основном связаны с продолжающимися усилиями компании по восстановлению поврежденных систем и услуг, а также с «решением некоторых других вопросов, возникших в результате инцидента».

CompuCom также ожидает, что часть расходов, понесенных после атаки программ-вымогателей, будет покрываться за счет киберстрахования.

«Компания осуществляет страхование, включая киберстрахование, которое, по ее мнению, соизмеримо с ее размером и характером операций, и ожидает, что часть этих расходов может быть покрыта страховкой», - добавила ODP Corporation.

MSP все еще работает над восстановлением предоставления услуг клиентам после того, как программа-вымогатель поразила его сеть, и ожидает «восстановления предоставления услуг практически всем своим клиентам» к концу марта.

Программа-вымогатель, развернутая с помощью маяков Cobalt Strike

Обнаружив, что операторы программы-вымогателя DarkSide начали шифрование систем CompuCom, MSP отключила их доступ к некоторым клиентам, чтобы заблокировать распространение вредоносного ПО.

Компания также уведомила клиентов о том, что они были скомпрометированы вредоносным ПО вскоре после атаки, но не предоставила никакой информации о возможной атаке вымогателя.

Пройдя первые этапы расследования инцидента, CompuCom обратилась к клиентам с «Часто задаваемыми вопросами для клиентов относительно инцидента с вредоносным ПО», содержащими дополнительную информацию.

Согласно часто задаваемым вопросам, злоумышленники установили маяки Cobalt Strike на нескольких системах в среде CompuCom, маяки, которые позволяли им красть данные, распространяться на другие сетевые устройства и в конечном итоге 28 февраля развертывать полезные нагрузки вымогателей…». ***(Sergiu Gatlan.***

CompuCom MSP expects over $20M in losses after ransomware attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/compucom-msp-expects-over-20m-in-losses-after-ransomware-attack/). 28.03.2021).

***

«Stratus Technologies подверглась атаке программы-вымогателя, потребовавшей отключения систем для предотвращения распространения атаки.

Stratus Technologies - известный поставщик продуктов высокой доступности, таких как их периферийные вычислительные устройства ztC и отказоустойчивое серверное решение ftServer. Продукты Stratus обычно используются банками, поставщиками телекоммуникационных услуг, центрами экстренного вызова и здравоохранением, которым требуется безотказная работа на уровне 99,999% (пять девяток).

Вчера Stratus Technologies сообщила, что они подверглись атаке с использованием программ-вымогателей, в результате чего они отключили отдельные части своей сети и служб, чтобы изолировать атаку.

«17 марта 2021 года компания Stratus Technologies, Inc. стала жертвой программы-вымогателя. Обнаружив подозрительную активность, мы отключили несколько систем, чтобы изолировать проблему, и приступили к реализации нашего плана обеспечения непрерывности бизнеса», - сообщила сегодня компания Stratus Technologies.

В рамках своего ответа Stratus также отключил свою ActiveService Network (ASN) и Stratus Service Portal.

Stratus ActiveService Network (ASN) - это услуга, предлагаемая с ее отказоустойчивыми продуктами, которая позволяет инженерам Stratus контролировать устройства по частным безопасным каналам связи. Эта услуга позволяет инженерам Stratus реагировать на проблемы или автоматически заменять вышедшие из строя детали, чтобы избежать простоев в системах заказчика.

Stratus заявляет, что они связались со всеми своими клиентами ASN для оказания дальнейшей поддержки…». ***(Lawrence Abrams. High-availability server maker Stratus hit by ransomware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/high-availability-server-maker-stratus-hit-by-ransomware/). 23.03.2021).***

***

Програми-трояни

«Новая кампания по распространению вредоносного спама заключается в злоупотреблении файлами значков, чтобы заставить жертв запустить троян NanoCore.

В четверг SpiderLabs в Trustwave сообщила, что недавняя фишинговая кампания обрисовала в общих чертах метод распространения трояна удаленного доступа (RAT) NanoCore.

Электронные письма якобы отправлены «менеджером по закупкам» организаций, которые подвергаются подделке, например, законных деловых партнеров. Эти фишинговые сообщения содержат вложение с именем «NEW PURCHASE ORDER.pdf * .zipx», которое на самом деле представляет собой двоичные файлы изображений. К значкам прикреплена дополнительная информация в формате .RAR. Используя файл значка, мошенники, вероятно, пытаются избежать безопасности и защиты, предлагаемой шлюзами электронной почты.

Если жертва нажимает на вложение и на ее ПК установлено средство разархивирования, такое как WinZip или WinRAR, исполняемый файл извлекается. 7Zip тоже может распаковать файл, но для этого потребуется не одна попытка.

«Нет необходимости переименовывать расширение недавних вложений во что-то другое, кроме .zipx или .zip, только для того, чтобы их исполняемые файлы были извлечены с помощью 7Zip», - говорят исследователи.

Успешное извлечение приводит к развертыванию NanoCore RAT версии 1.2.2.0. Этот троян удаленного доступа (RAT), впервые обнаруженный в 2013 году, включает в себя кейлоггер, программу для кражи информации, дроппер для дополнительных вредоносных программ, а также содержит возможность доступа и кражи видеозаписей с веб-камеры, а также эксфильтрации данных для отправки в команду и -управление (C2) сервером.

Вредоносная программа ранее продавалась на подпольных форумах и часто распространяется через фишинговые кампании финансового характера.

Эта версия троянца может создавать свои копии в папке AppData, а также компрометирует процесс RegSvcs.exe. Информация, украденная вредоносным ПО, отправляется нескольким C2.

Методика, отмеченная SpiderLabs, похожа на прошлую фишинговую кампанию, в которой также использовались файлы .zipx. В 2019 году исследователи сообщили в своем блоге, что Lokibot, еще один троянец, который также может взламывать криптовалютные кошельки, распространялся в кампаниях по борьбе со спамом через расширение .zipx и значки .JPG». ***(Charlie Osborne. Icon files abused in malspam to spread NanoCore Trojan // ZDNet (https://www.zdnet.com/article/icon-files-abused-in-malspam-to-spread-nanocore-trojan/). 11.03.2021).***

***

«Кибератаки, стоящие за кампаниями ObliqueRAT, теперь маскируют троян в безобидных файлах изображений на взломанных веб-сайтах.

Троян удаленного доступа ObliqueRAT (RAT), обнаруженный в начале 2020 года, восходит к атакам на организации в Южной Азии.

При первом обнаружении вредоносная программа была описана как "простая" RAT с типичными основными функциями трояна, ориентированными на кражу данных, такими как способность извлекать файлы, подключаться к серверу управления и контроля (C2), и возможность завершить существующие процессы. Вредоносная программа также может проверять наличие любых признаков, указывающих на то, что ее цель находится в изолированной программной среде,

что является обычной практикой, которую инженеры по кибербезопасности используют в образцах вредоносного ПО для обратного проектирования.

С момента своего первоначального открытия ObliqueRAT был модернизирован новыми техническими возможностями и использует более широкий набор исходных векторов заражения. В сообщении в блоге во вторник Cisco Talos сообщила, что новая кампания, разработанная для развертывания RAT в том же регионе, изменила способ обслуживания вредоносного ПО в системах-жертвах.

Раньше документы Microsoft Office отправлялись через фишинговые сообщения электронной почты на цель, содержащую вредоносные макросы, что приводило к прямому развертыванию ObliqueRAT. Однако теперь эти вредоносные программы вместо этого направляют жертв на вредоносные веб-сайты - вероятно, в попытке обойти меры безопасности электронной почты.

Применяется метод, известный как стеганография. Стеганография используется для сокрытия кода, файлов, изображений и видеоконтента внутри другого содержимого файловых форматов, и в этом случае исследователи обнаружили файлы .BMP, содержащие вредоносные полезные данные ObliqueRAT.

Эти файлы .BMP размещены на веб-сайтах, которые были взломаны злоумышленниками. Хотя файлы действительно содержат допустимые данные изображения, исполняемые байты также скрыты в данных RGB - и при просмотре запускают загрузку файла .ZIP, содержащего ObliqueRAT.

По словам исследователей, вредоносные макросы, содержащиеся в maldoc, извлекают файл архива и развертывают трояна в целевой системе конечных точек.

В общей сложности недавно были обнаружены четыре новые версии вредоносного ПО, которые, по всей видимости, были разработаны в период с апреля по ноябрь 2020 года. Улучшения включают проверку конечных точек в заблокированном списке и имен компьютеров, а также включение возможности извлечения файлов из внешнего хранилища. Новая командная строка, еще не назначенная, также указывает на то, что в будущем произойдут дополнительные обновления.

ObliqueRAT также был связан с кампаниями по распространению CrimsonRAT. Есть потенциальные связи с Transparent Tribe (.PDF), спонсируемая государством группа угроз Proofpoint утверждает, что ранее атаковала посольства Индии в Саудовской Аравии и Казахстане. Из-за дублирования инфраструктуры C2 также могут быть связи с кампаниями RevengeRAT». ***(Charlie Osborne. ObliqueRAT Trojan now lurks in images on compromised websites // ZDNet (https://www.zdnet.com/article/obliquerat-trojan-now-hides-in-images-on-compromised-websites/). 02.03.2021).***

***

«Недавний срыв Emotet, управляемый всемирной коалицией правоохранительных органов, имеет огромное значение. Существуют очевидные последствия для кибербезопасности, связанные с нарушением так называемого «самого опасного вредоносного ПО в мире», но также это является сильным напоминанием о важности сотрудничества между общественностью и частным сектором в борьбе с киберпреступностью. Удаление Netwalker и Egregor - дополнительные примеры, еще больше подчеркивающие необходимость такого типа координации.

Удаление вредоносного ПО

В январе Европол объявил, что всемирная коалиция правоохранительных органов США, Канады, Великобритании, Нидерландов, Германии, Франции, Литвы и Украины разрушила Emotet, известную как самое опасное вредоносное ПО в мире. Глобальные усилия, известные как операция «Божья коровка», также включали координацию с частными исследователями безопасности. Вместе они смогли взять под контроль инфраструктуру ботнета.

Другая крупная кибер-акция, объявленная в конце января Министерством юстиции США, также включала скоординированные международные усилия правоохранительных органов. Их целью была программа-вымогатель NetWalker, которая затронула множество жертв в разных секторах, включая компании, школы, больницы и муниципалитеты, с атаками, специально нацеленными на сектор здравоохранения во время пандемии COVID-19. Власти предъявили обвинение одному человеку и изъяли почти полмиллиона долларов в криптовалюте от выкупа.

В рамках совместной операции Украины, Франции и США власти разогнали группу киберпреступников, связанную с Egregor, которая использует преступные организации для проведения атак с применением программ-вымогателей. Власти преследовали как лидеров группировки, так и ее филиалы, и произвели несколько арестов; в результате операции был нарушен веб-сайт группы и командный сервер.

Все эти кейсы - прекрасные примеры необходимости усиления координации, когда речь идет о кибербезопасности. Прогресс есть, но нам нужно больше, и это срочно.

Глобальная проблема кибербезопасности

Киберпреступность не имеет границ, поэтому ее сложно отследить и остановить. Сегодняшние глобальные сетевые инфраструктуры соединяют различные группы через единую взаимосвязанную структуру. Это упрощает межведомственное сотрудничество, но позволяет киберпреступникам выходить за пределы границ и наносить удары по жертвам так, как не могут правоохранительные органы. Как показывают последние тенденции в области угроз, кибер-злоумышленники все чаще нацеливаются на постоянно растущий диапазон цифровых атак с помощью разрушительных кибератак.

Такая глобальная взаимосвязанность ставит каждого перед лицом проблем, создаваемых самыми слабыми звеньями всемирной киберцепи. Она еще больше

усугубляет проблемы экстрадиции и убежища, давние препятствия для международных уголовных расследований любого рода. Расследованию киберпреступлений в одних странах помешал отказ других стран ответить взаимностью в плане экстрадиции. И это не говоря уже о возможностях и недостатке обучения; многие муниципальные организации борются с ограниченным бюджетом, который не позволяет им располагать кадрами и навыками, которые им необходимы в этом отношении.

Частный и государственный секторы должны объединиться

Однако это не только вопрос правоохранительных органов. Частный сектор также может сыграть ключевую роль. Чтобы действительно решить проблемы кибербезопасности, которые продолжают трансформироваться и расти, частный сектор должен сотрудничать с правоохранительными органами. Сюда входят такие организации, как Интерпол и ФБР, а также местные агентства и департаменты, мировые системы уголовного правосудия стран.

Преимущество частного сектора заключается в его способности выявлять, отслеживать и анализировать инфраструктуру и сервисы киберпреступников. Это дает более качественную техническую информацию, которой частный сектор может делиться и использовать. Специалисты частного сектора могут обнаруживать преступную деятельность и целенаправленно нарушать работу преступной инфраструктуры. Но у них нет всей информации - или правоприменения. Именно здесь правительство может вмешаться, чтобы преследовать киберпреступников и оштрафовать. У государственного и частного секторов нет всего, что им нужно, чтобы остановить киберпреступность; они должны работать вместе.

…Трудно поместить необработанную информацию в более широкий контекст информации о злоумышленниках - кто, что, когда, где и как. В нашу эпоху больших данных любая передаваемая информация также должна подходить для автоматизации, и не у всех есть опыт обмена информацией такого типа.

Кроме того, обмен информацией должен быть быстрым, идти в ногу с движением злоумышленника или опережать его, что часто являлось слабым звеном государственно-частного сотрудничества. Информации тоже нужно доверять, особенно при работе с автоматизацией. И, наконец, проблемы с конфиденциальностью и неприкосновенностью частной жизни еще больше усложняют ситуацию - но с этим можно справиться путем обмена только неперсонально идентифицируемой информации.

Итеративная совместная безопасность

Есть еще много угроз глобального масштаба, откуда пришли Emotet и Netwalker. Государственный и частный секторы хорошо работали вместе через границы, чтобы подорвать эти две деструктивные силы. Каждая сторона государственно-частного сотрудничества имеет ресурсы и возможности, которые поддерживают другую и повышают эффективность борьбы с киберпреступностью. Проблемы обмена информацией остаются, но процессы сотрудничества будут улучшаться по мере появления большего числа таких партнерств. Организации будут учиться друг у друга и на опыте прошлого сотрудничества в процессе непрерывного совершенствования, которое изменит баланс сил в пользу хороших

парней». ***(Derek Manky. Ransomware Takedowns Underscore Need for Private-Public Cybersecurity Collaboration // Wired Business Media (https://www.securityweek.com/ransomware-takedowns-underscore-need-private-public-cybersecurity-collaboration). 05.03.2021).***

***

«По словам официальных лиц, подросток из Флориды, обвиненный в организации взлома аккаунтов знаменитостей в Твиттере в рамках криптовалютной схемы, был приговорен к трем годам тюремного заключения для несовершеннолетних по соглашению о признании вины.

Во вторник государственная прокуратура объявила о сделке по делу 18-летнего Грэма Ивана Кларка, названного вдохновителем всемирного взлома Bit-Con в июле 2020 года на аккаунты Твиттера Илона Маска, Билла Гейтса, Барака Обамы, Джо Байдена и других.

Прокурор округа Хиллсборо Эндрю Уоррен сказал, что Кларк, которому было 17 лет, когда ему было предъявлено обвинение, будет отбывать три года в тюрьме для несовершеннолетних с последующим трехлетним испытательным сроком - максимум, разрешенный Законом Флориды о несовершеннолетних правонарушителях.

Если Кларк нарушит свой испытательный срок, ему грозит минимум 10 лет тюремного заключения для взрослых.

Взлом, в результате которого были выдвинуты федеральные обвинения против трех других людей, захватил учетные записи знаменитостей и попросил их последователей отправить биткойны на счет, пообещав удвоить их деньги…

Уоррен добавил, что «наша цель с любым ребенком, когда это возможно, - заставить его усвоить урок, не разрушая его будущее», и предлагает ему шанс на реабилитацию.

Дело расследовали федеральные власти, но Кларк был передан штату, так как в то время он был несовершеннолетним.

По словам прокуратуры, Кларк использовал свой доступ к внутренним системам Твиттера, чтобы получить доступ к учетным записям нескольких компаний и знаменитостей, и совершил комбинацию «технических нарушений и социальной инженерии», заработав около 100 000 долларов.

Twitter заявил тогда, что инцидент 15 июля произошел в результате атаки «целевого фишинга», в результате которой сотрудники были обмануты относительно происхождения сообщений.

Взлом затронул как минимум 130 аккаунтов, в том числе аккаунт Байдена, когда он был кандидатом в президенты». ***(US Teen 'Mastermind' in Epic Twitter Hack Sentenced to Prison // Wired Business Media (https://www.securityweek.com/florida-teen-sentenced-hack-celebrity-twitter-accounts). 17.03.2021).***

****

«Роберт Пурбек из Меридиана, штат Айдахо, впервые предстал перед мировым судьей США в Бойсе, штат Айдахо. Пурбек был обвинен в Северном

округе Джорджии 2 марта 2021 года в компьютерном мошенничестве и злоупотреблениях, мошенничестве с устройствами доступа и мошенничестве с использованием электронных средств.

«Этот предполагаемый киберпреступник и вымогатель нацелился на город Ньюнан, а также на медицинские клиники в нашем округе, похитив более 60 000 записей, содержащих личную информацию наших граждан», - сказал исполняющий обязанности прокурора США Курт Р. Эрскин. «Затем он якобы пытался вымогать у ортодонта из Флориды, угрожая продать номер социального страхования своего несовершеннолетнего ребенка, если ортодонт не предъявит требование о выплате. Теперь этот обвиняемый должен ответить за свои предполагаемые преступления в Северном округе Джорджии».

«Обвинения против Пурбека подчеркивают необходимость сохранять бдительность в наших усилиях по обеспечению кибербезопасности», - сказал Крис Хакер, специальный агент, отвечающий за ФБР в Атланте. «Кража интеллектуальной собственности с целью вымогательства у граждан - очень серьезное преступление, и ФБР будет его усердно преследовать, независимо от того, прячетесь ли вы за экраном компьютера».

По словам исполняющего обязанности прокурора США Эрскина, обвинения и другая информация были представлены в суде: в период с 23 июня 2017 года по 28 апреля 2018 года Пурбек якобы приобрел на криминальном рынке имя пользователя и пароли к компьютерным серверам, принадлежащим нескольким жертвам в Джорджии. Затем он предположительно использовал эти учетные данные для доступа к компьютерам жертв и украл конфиденциальную личную информацию, в том числе:

Медицинские записи и другие документы, содержащие имена, адреса, даты рождения и номера социального страхования более 43 000 человек из медицинской клиники в Гриффине, штат Джорджия;

Полицейские отчеты и другие документы, содержащие личную информацию о более чем 14 000 человек из города Ньюнан; и

Личная информация более 7000 человек из Locust Grove, Джорджия, медицинская практика.

25 июня 2018 года Пурбек якобы взломал компьютеры ортодонта во Флориде и украл медицинские записи более 1800 человек. Затем Пурбек якобы угрожал, преследовал и пытался вымогать у ортодонта, требуя выкуп в биткойнах. Пурбек также якобы угрожал раскрыть и продать украденную информацию о пациенте и личную информацию, если ортодонт не оплатит требование выкупа. Пурбек якобы идентифицировал имя и номер социального страхования несовершеннолетнего ребенка ортодонта, а также угрожал раскрыть и продать их личную информацию. В ходе этой попытки вымогательства Пурбек якобы отправлял ортодонту и его пациентам многочисленные беспокоящие электронные письма и текстовые сообщения.

Роберт Пурбек, a / k / a Lifelock, a / k / a Studmaster, 41 год, из Меридиана, штат Айдахо, был обвинен федеральным большим жюри в Северном округе Джорджии 2 марта 2021 года. Напоминаем членам общественности, что обвинительное заключение содержит только обвинения. Подсудимый считается

невиновным по предъявленным обвинениям, и правительство должно будет доказать вину обвиняемого вне разумных сомнений в суде.

Этот случай расследуется Федеральным бюро расследований, Полевой офис в Атланте, при неоценимой помощи со стороны резидентского агентства ФБР в Бойсе.

Помощник прокурора США Майкл Херсковиц, начальник отдела преступлений в сфере киберпреступлений и интеллектуальной собственности, и Натан Китченс, начальник отдела общественной честности и особых вопросов, а также Отдел компьютерных преступлений и интеллектуальной собственности Министерства юстиции США (CCIPS) ведут судебное преследование. Прокуратура США по округу Айдахо также оказала ценную помощь в этом деле». ***(Idaho man charged with hacking into the computers of the City of Newnan and metro-Atlanta medical clinics // Department of Justice (https://www.justice.gov/usao-ndga/pr/idaho-man-charged-hacking-computers-city-newnan-and-metro-atlanta-medical-clinics). 05.03.2021).***

***

«Sky ECC утверждает, что копы взломали поддельную версию приложения, выдаваемую недовольным реселлером.

Европол начал «серьезные вмешательства» против организованной преступности 9 марта, что, по его словам, стало возможным благодаря отслеживанию зашифрованных сообщений около 70 000 пользователей службы Sky ECC с середины февраля.

Sky ECC, которая занимается продажей мобильных телефонов со специализированной частной связью, отрицает, что сообщения на ее платформе были расшифрованы. Однако массовые аресты в Бельгии, Франции и Нидерландах, о которых сообщил Европол в сотрудничестве с правоохранительными органами этих стран, похоже, указывают на иное. А Европол заявил, что с собранными данными еще не сделано, что, как он надеется, приведет к дополнительным действиям и судебным преследованиям.

Европол сообщил, что у Sky ECC около 170 000 пользователей, которые отправляют около 3 миллионов сообщений каждый день, добавив, что 20% этих пользователей находятся в Бельгии и Нидерландах.

«Благодаря успешной разблокировке шифрования Sky ECC, полученная информация предоставит представление о преступной деятельности в различных государствах-членах ЕС и за его пределами, а также поможет в расширении расследований, раскрытии серьезных и трансграничных организованных преступлений в ближайшие месяцы, а возможно, и годы. »- говорится в сообщении Европола.

Последняя операция последовала за крахом EncroChat в июле прошлого года, когда Национальное агентство по борьбе с преступностью Великобритании захватило серверы службы и прекратило деятельность организованной преступности, проводившуюся с помощью зашифрованных сообщений, включая отмывание денег, где прятать наркотики и даже убийства. По данным Европола, в

ходе этого перерыва было произведено более 700 арестов, а оставшиеся клиенты перешли в Sky ECC.

В этом месяце репрессии начались в Бельгии, когда полиция изъяла устройства у подозреваемых, которые, как выяснилось, использовали Sky ECC для организации и общения.

Только в Бельгии в операциях участвовало более 1600 бельгийских полицейских, некоторые из которых сопровождались спецназом, и были совершены рейды на 200 жилых домов.

Голландская полиция сообщила, что они провели 75 обысков в домах, арестовали 30 подозреваемых и изъяли миллионы наличными, восемь автомобилей, оружие, банкоматы и полицейскую форму.

В заявлении правоохранительных органов Нидерландов от 9 марта говорится, что операция под названием «Аргус» включала захват серверов Sky ECC.

Sky ECC отрицает расшифровку сообщений

Sky ECC опровергает факт взлома сообщений, размещая на своей домашней странице уведомление: «Голландская полиция подтверждает, что они расследуют поддельный телефон Sky ECC», - заявила компания. «Этот телефон был разработан кем-то, кто уже несколько лет выдает себя за официального реселлера».

Торгового посредника называют SKYECC.EU, и Sky ECC предоставила фотографии телефона, конфискованного голландскими властями, для сравнения с подлинным телефоном Sky ECC.

«Этот телефон «E.U.» не принадлежит нам и не продается нами», - говорит Жан-Франсуа Иап, генеральный директор Sky ECC. «Мы знаем, что кто-то выдает себя за официального реселлера Sky ECC в течение некоторого времени, и мы пытаемся закрыть его через легальные каналы в течение почти двух лет».

Sky ECC заявляет, что настолько уверена в своей безопасности, что предлагает приз в размере 5 миллионов долларов каждому, кто сможет их взломать. Компания также отрицала, что какие-либо правоохранительные органы, стоявшие за этой недавней облавой, просили выплату.

«Власти не связывались со Sky ECC в связи с расследованиями, о которых в настоящее время сообщается», - сказал Иап. «Запутанные ссылки на Sky ECC вместо SKYECC.EU очень разрушительны. Если власти основывают какую-либо оценку Sky ECC на SKYECC.EU, они серьезно ошибаются в отношении характера Sky ECC и его операций».

Иап добавил, что компания активно работает над этой проблемой.

Вымерли частные коммуникации?

«С одной стороны, трудно поверить, что такая организация, как Европол, сделает ложное или преувеличенное заявление, но это может быть тактика, которую они используют, чтобы подтолкнуть преступников к менее защищенной платформе или той платформе, на которую у них есть больше крючков», - сказал Хоффман. «С другой стороны, операторы Sky ECC столкнулись бы с крахом всей своей бизнес-модели, если бы у них возникла эта проблема, и, естественно, они сделали все, что в их силах, чтобы обмен сообщениями оставался безопасным».

Вопрос в том, сколько клиентов Sky ECC готовы сделать ставку на то, блефует ли Европол? Или многие просто перейдут на другую службу

зашифрованных сообщений, как это было при миграции с EncroChat прошлым летом?

Тим Уэйд, который работает в компании Vectra, что захват или перехват личных сообщений правоохранительными органами для любых целей следует рассматривать как опасное нарушение основных прав.

«Частное общение необходимо для свободного и справедливого общества», - сказал Уэйд. «Обойдя обоснованность утверждений о компрометации Sky ECC, очень важно, чтобы мы признали, что преступники, злоупотребляющие шифрованием, - это цена, которую стоит заплатить за обеспечение личной конфиденциальности и пользоваться преимуществами, которые такая конфиденциальность дает нашей культуре». ***(Becky Bracken. Europol Credits Sweeping Arrests to Cracked Sky ECC Comms // Threatpost (https://threatpost.com/europol-arrests-cracked-sky-ecc/164744/). 12.02.2021).***

***

«Россиянин Егор Крючков на суде в США признал себя виновным в попытке организовать кибератаку на компьютерную сеть компании Tesla в штате Невада. Ранее он отрицал свою причастность к этому делу, а его родственники говорили, что Крючков не имеет отношение к сфере информационных технологий и никогда не занимался программированием.

«Гражданин России сегодня в федеральном суде признал вину в сговоре с целью поездки в США для вовлечения сотрудника компании в Неваде в схему по внедрению вредоносного программного обеспечения в компьютерную сеть компании», — подтвердили в Минюсте США. Приговор Егору Крючкову должны вынести 10 мая.

По версии Минюста США, Егор Крючков намеревался завербовать сотрудника компании Tesla из Невады, чтобы тот установил вредоносное программное обеспечение, позволяющее взломать компьютерную сеть. Россиянин пообещал вознаграждение в 1 млн долларов. План хакеров был сорван самим сотрудником предприятия, который обратился в ФБР.

Как сообщается, россиянин планировал похитить данные из сети Tesla, чтобы потом вымогать за них деньги. Схему пресекло ФБР, задержав Крючкова 22 августа в Лос-Анджелесе». ***(Россиянин Крючков признал вину в подготовке кибератаки на завод Tesla // SecurityLab.ru (https://www.securitylab.ru/news/517580.php). 19.03.2021).***

***

«В четверг суд Джорджии приговорил к тюремному заключению 22-летнего Джошуа Пеллосо Эпифанию, который был арестован на Кипре в мае 2017 года и в прошлом году стал первым гражданином Кипра, выданным Соединенным Штатам.

«Эта историческая экстрадиция и вынесение приговора были бы невозможны без решимости наших следователей ФБР и помощи наших федеральных и иностранных партнеров», - сказал Крис Хакер, специальный агент ФБР в Атланте, штат Джорджия, в заявлении Министерства юстиции.

«Это еще одно доказательство того, что независимо от того, где скрываются преступники, которые охотятся на компании и граждан США, географически или виртуально, мы будем преследовать их и предавать правосудию», - сказал Хакер.

Кипрский адвокат Майкл Чемберс в электронном письме AFP сказал, что апелляция не будет подана, хотя Эпифаниу признался и ожидал, что его освободят вовремя.

«Я не считаю, что приговор стоит обжаловать, поскольку он будет освобожден через 10 месяцев», - сказал Чемберс.

Команда юристов Кипра надеялась, что Эпифаниу будет освобожден, поскольку он признал себя виновным и выплатил компенсацию.

Эпифаниу признал себя виновным по федеральным обвинениям в компьютерном мошенничестве, выдвинутым в Аризоне и Джорджии.

В результате осуждения Эпифаниу конфисковал 389 113 долларов США и 70 000 евро (83 000 долларов США) в пользу правительства и выплатил 600 000 долларов в качестве возмещения своим жертвам мошенничества за счет полученной им криптовалюты.

Эпифаниу был экстрадирован 16 июля прошлого года по обвинению в преступлениях, совершенных ночью из его спальни в доме его матери в Никосии, когда он был подростком.

Максимальный срок лишения свободы по предъявленным ему обвинениям составлял 20 лет.

В период с октября 2014 года по май 2017 года Epifaniou взламывал веб-сайты и отслеживал онлайн-трафик для выявления целей вымогательства.

После выбора целевых веб-сайтов он работал с сообщниками, чтобы украсть информацию из баз данных веб-сайтов.

Затем Epifaniou использовал прокси-серверы, расположенные в зарубежных странах, для входа в учетные записи электронной почты и отправки сообщений на веб-сайты с угрозами утечки конфиденциальных данных, если выкуп не будет выплачен в биткойнах, стоимость которых с тех пор резко выросла.

Первоначально арестованный в Никосии в возрасте 17 лет, он провел более трех лет в кипрской тюрьме, не будучи осужденным и не борясь с экстрадицией…». ***(Defense of Convicted Cypriot Hacker in US Not Seeking Appeal // Wired Business Media (https://www.securityweek.com/defence-convicted-cypriot-hacker-us-not-seeking-appeal). 22.06.2021).***

***

«Бывший ИТ-подрядчик был приговорен к двум годам тюремного заключения за взлом сервера компании и удаление большинства учетных записей Microsoft Office 365 (O365) ее сотрудников. В результате инцидента компания полностью остановилась на два дня.

32-летний подрядчик, Дипаншу Кхер, изначально работал в неназванной консалтинговой ИТ-фирме с 2017 по май 2018 года. В 2017 году консалтинговая фирма была нанята неназванной компанией в Карлсбаде, Калифорния, чтобы помочь с ее переходом на Окружение O365 - и отправил Хера помочь с проектом.

Однако, согласно сообщению Министерства юстиции (DoJ) в понедельник, компания была недовольна работой Хера. Кхера вывели из проекта в 2018 году, а через несколько месяцев уволили из консалтинговой фирмы.

8 августа 2018 года Кхер взломал сервер компании и удалил более 1200 из 1500 учетных записей пользователей O365. По данным Министерства юстиции, атака затронула большую часть сотрудников компании и полностью закрыла компанию.

«Учетные записи сотрудников были удалены - они не могли получить доступ к своей электронной почте, спискам контактов, календарям встреч, документам, корпоративным каталогам, видео- и аудиоконференциям, а также к виртуальной среде Teams, необходимой им для выполнения своей работы», - сообщает Министерство юстиции США. «За пределами компании клиенты, поставщики и потребители не могли связаться с сотрудниками компании (и сотрудники не могли связаться с ними). Никто не мог сообщить этим покупателям, что происходит или когда компания снова начнет работать».

Даже по прошествии этих двух дней проблемы у сотрудников компании не исчезли. Например, сотрудники не получали приглашения на собрания, их списки контактов не могли быть полностью перестроены, и они больше не могли получить доступ к определенным папкам, к которым у них был ранее доступ.

Кхер, гражданин Индии, который вернулся в Индию в 2018 году до совершения взлома, был арестован, когда вылетал из Индии в США 11 января. Согласно Министерству юстиции, он не знал об ордере на его арест.

В дополнение к двум годам тюремного заключения судья окружного суда США приговорил Кхера к трем годам контролируемого освобождения и приказал вернуть компании 567 084 доллара (сумма, которую компания заплатила для устранения проблем, вызванных взломом).

Следует отметить, что максимальное наказание за преступление, за которое был осужден Хер («умышленное повреждение защищенного компьютера»), составляет 10 лет лишения свободы.

Этот инцидент является ярким напоминанием о разрушительном воздействии, которое «инсайдерские угрозы» - будь то недовольные сотрудники, сторонний подрядчик или что-то еще - могут оказать на безопасность и конфиденциальность данных компании.

В декабре мужчина был приговорен к двум годам тюремного заключения по обвинению во взломе платформы Cisco Webex для совместной работы в деле об инсайдерской угрозе, переданном в Окружной суд США в Калифорнии.

И в другом аналогичном инциденте, массовом взломе Capital One в 2019 году, затронувшем более 100 миллионов человек в США и 6 миллионов в Канаде, был виноват бывший инженер Amazon Web Services (AWS), который работал с компанией, который предположительно похвастался кражей данных на GitHub.

Рик Холланд, директор по информационной безопасности и вице-президент по стратегии Digital Shadows, сказал, что для борьбы с такими рисками внутренних угроз организациям следует проводить оценку рисков внутренних угроз для своих критически важных бизнес-функций, которые могут быть использованы инсайдерами для совершения мошенничества.

«Самая серьезная сложность в борьбе с внутренней угрозой в сегодняшнем мире удаленной рабочей силы заключается в том, что средства управления безопасностью, предназначенные для отслеживания и отслеживания активности, могут быть не такими эффективными, как в традиционном локальном мире», - сказал Холланд». ***(Lindsey O'Donnell. Office 365 Cyberattack Lands Disgruntled IT Contractor in Jail // Threatpost (https://threatpost.com/office-365-cyberattack-disgruntled-contractor-jail/164986/). 23.03.2021).***

***

Злам Microsoft Exchange

«По данным Microsoft, около 80 000 серверов Exchange еще не получили исправлений для активно используемых уязвимостей.

Об этих ошибках стало известно 2 марта, когда технический гигант из Редмонда объявил не только об исправлениях для них, но и о том, что китайский злоумышленник активно использовал их в атаках.

В течение нескольких дней исследователи безопасности обнаружили, что несколько злоумышленников быстро подобрали эксплойты для ошибок Exchange, некоторые из которых нацелились на недостатки еще до выпуска исправлений. Первая известная попытка эксплуатации датирована 3 января, за 58 дней до публичного раскрытия информации.

В течение прошлой недели Microsoft выпустила дополнительные исправления для этих уязвимостей, включая обновления безопасности (SU) для старых и неподдерживаемых версий Exchange Server или накопительные обновления (CU), как их называет компания.

«Это задумано только как временная мера, чтобы помочь вам защитить уязвимые компьютеры прямо сейчас. Вам по-прежнему необходимо обновиться до последней поддерживаемой версии CU, а затем применить соответствующие SU», - заявили в Microsoft.

С последним набором выпущенных обновлений охвачено более 95% версий Exchange Server, доступных в Интернете, но десятки тысяч компьютеров остаются уязвимыми. Microsoft сообщила, что по состоянию на 12 марта более 82 000 серверов Exchange все еще нуждались в обновлении (из 400 000, выявленных 1 марта).

На прошлой неделе ESET сообщила, что более 10 злоумышленников нацелены на уязвимые серверы Exchange. Операторы программ-вымогателей также начали нацеливаться на недостатки, и общее количество атак, направленных на нулевые дни Exchange, выросло экспоненциально всего за несколько дней.

В воскресенье исследователи безопасности из Check Point отметили, что «количество попыток использования уязвимостей увеличилось более чем в 6 раз» «только за последние 72 часа», добавив, что они выявили более 4800 эксплойтов и сотни взломанных организаций по всему миру.

Больше всего преследовали Соединенные Штаты, на которые приходилось 21% всех попыток эксплуатации, за ними следуют Нидерланды и Турция - по 12%.

По данным Check Point, правительственный / военный сектор был наиболее уязвимым сектором (27% попыток), за ним следовали производство (22%) и программное обеспечение (9%).

«Поскольку мы переходим во вторую неделю с момента обнародования уязвимостей, по первоначальным оценкам количество взломанных организаций исчисляется десятками тысяч», - заявила на прошлой неделе Palo Alto Networks.

В хронологии атак компания по безопасности показала, что первые две ошибки были обнаружены 10 и 30 декабря 2020 года, соответственно, и о них было сообщено в Microsoft 5 января 2021 года. Третья дыра в безопасности была обнаружена и сообщена, когда она уже подверглась атаке, 27 января.

«Текущие исследования показывают, что эти уязвимости используются несколькими группами угроз. Хотя для высококвалифицированных злоумышленников не в новинку использовать новые уязвимости в различных экосистемах продуктов, способы, которыми эти атаки осуществляются для обхода аутентификации - тем самым обеспечивая несанкционированный доступ к электронной почте и позволяя удаленное выполнение кода (RCE), - особенно гнусны», Отметила Palo Alto Networks…». ***(Ionut Arghire. Over 80,000 Exchange Servers Still Affected by Actively Exploited Vulnerabilities // Wired Business Media (https://www.securityweek.com/over-80000-exchange-servers-still-affected-actively-exploited-vulnerabilities?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Securityweek+%28SecurityWeek+RSS+Feed%29). 15.03.2021).***

***

«В этом месяце исследовательская компания по кибербезопасности Volexity обнаружила серию из четырех критических уязвимостей в программном обеспечении Microsoft Exchange Server. С тех пор уязвимость была независимо проверена и подтверждена Microsoft. Считается, что она использовалась иностранными государственными субъектами угроз в течение неизвестного периода времени, по крайней мере, до января 2021 года. Exchange действует как серверное программное обеспечение, которое обрабатывает электронную почту для подавляющего большинства крупных организаций; Outlook подключается к Exchange для отображения электронной почты для учетных записей пользователей.

Хотя уязвимость не затрагивает клиентов, использующих исключительно службу Microsoft Exchange Online, большинство организаций в США используют ту или иную форму Microsoft Outlook Web Access (OWA) с выходом в Интернет для своих систем электронной почты в тандеме с серверами Exchange.

Компании, которые используют Microsoft Exchange Server для обмена сообщениями электронной почты в любой версии, должны немедленно предпринять шаги для решения этой проблемы. Office 365 не затронут, но компании с физическими серверами Exchange в сочетании с Office 365 по-прежнему будут уязвимы. Уязвимость затрагивает каждую версию Microsoft Exchange Server с 2010 по 2016 год. Эксплуатируемая уязвимость и потенциальный «черный ход» позволяют удаленному злоумышленнику получить полный доступ и

контроль над сервером Exchange организации, включая все данные, хранящиеся на нем - электронные письма, вложения, контакты, заметки, задачи, элементы календаря и т. д. Злоумышленники, использующие уязвимость, также могут идентифицировать почтовый ящик по имени пользователя и просматривать или копировать все содержимое почтового ящика.

Серьезность вопроса трудно переоценить. Используя эксплойт, злоумышленники могут оставить один или несколько сценариев «веб-оболочки» для использования в будущем. Веб-оболочка - это простой в использовании, защищенный паролем хакерский инструмент, к которому можно получить доступ из любого браузера через Интернет. Он также обычно используется для важных функций, и поэтому его сложно идентифицировать как вредоносное ПО только по типу файла.

На данный момент среди пострадавших есть предприятия, местные органы власти, строительные компании, больницы и финансовые учреждения, включая Европейское банковское управление. Количество затронутых организаций исчисляется десятками тысяч. Кроме того, ожидается, что список затронутых компаний значительно расширится по мере того, как все больше людей узнают о проблеме, исследуют трафик и активность серверов.

Текущая информация предполагает, что злоумышленником (хакером) в этом случае была китайская кибершпионажная группа под названием Hafnium, основной целью которой является кража информации организаций. Хотя 2 марта 2020 года Microsoft выпустила патч для исправления этих уязвимостей, злоумышленники, создавшие угрозу Hafnium, резко активизировали свои действия в ответ, надеясь захватить организации, которые не знали о патче. Их увеличение атак, кажется, работает.

Президент Volexity Стивен Адэр сказал: «Даже если вы установили исправления в тот же день, когда Microsoft опубликовала свои исправления, все равно высока вероятность, что на вашем сервере есть веб-оболочка. На самом деле, если вы используете Exchange и еще не установили патч, высока вероятность того, что ваша организация уже взломана».

Что еще хуже - с тех пор, как были объявлены уязвимость и патчи, другие хакеры спешили воспользоваться ситуацией и установить собственные файлы Web Shell. И чем больше времени требуется организациям-жертвам, чтобы удалить бэкдоры, тем более вероятно, что злоумышленники последуют, установив дополнительные бэкдоры или даже расширив свою атаку, чтобы включить другие части сетевой инфраструктуры жертвы.

По состоянию на 5 марта, по самым скромным оценкам, пострадало 30 000 или более организаций. Считается, что по состоянию на 8 марта это число увеличилось вдвое и составило 60 000 человек. Несомненно, на момент написания этой статьи их число было еще больше: тысячи серверов были скомпрометированы за час во всем мире. Официальные лица США сообщили CNN, что около четверти миллиона организаций находятся в опасности или уже взломаны в результате использования этих уязвимостей.

Microsoft сообщила, что она сотрудничает с Агентством кибербезопасности и безопасности инфраструктуры США (CISA), а также с другими

правительственными агентствами и компаниями, занимающимися безопасностью, чтобы гарантировать своим клиентам наилучшие рекомендации и меры по снижению рисков. CISA выпустила чрезвычайную директиву, предписывающую всем федеральным гражданским ведомствам и агентствам, использующим уязвимые серверы Microsoft Exchange, либо обновить программное обеспечение, либо отключить продукты от своей сети.

Эта критическая проблема будет иметь долгосрочные последствия и повлияет на весь мир. Кроме того, отсутствие групп реагирования на инциденты - по сравнению с количеством атакованных организаций - вызывает острую нехватку спроса компетентных специалистов по кибербезопасности для устранения огромного количества нарушений, вызванных этой уязвимостью.

Если вы обеспокоены тем, что ваша организация может использовать Microsoft Exchange и Outlook Web Access, и вам нужна помощь в оценке собственной ситуации в вашей организации, мы рекомендуем вам обратиться к специалистам по кибербезопасности Seyfarth, которые помогут вам немедленно реагировать на угрозы, смягчить их последствия и соблюдать правовые нормы». ***(Richard Lutkus, Jason Priebe, Emily Dorner. ORGANIZATIONS USING MICROSOFT EXCHANGE MAIL SERVER FACE SEVERE CYBERSECURITY THREAT // Seyfarth Shaw LLP (https://www.carpedatumlaw.com/2021/03/organizations-using-microsoft-exchange-mail-server-face-severe-cybersecurity-threat/#page=1). 12.03.2021).***

***

«Агентство по кибербезопасности и безопасности инфраструктуры (CISA) издало сегодня чрезвычайную директиву (ED) 21-02, требующую от федеральных гражданских ведомств и агентств, использующих локальные продукты Microsoft Exchange, обновлять или отключать продукты от своих сетей до тех пор, пока не будет выпущен патч Microsoft… Это также требует от агентств, которые в настоящее время могут это делать, для сбора криминалистических изображений. Все агентства также должны искать известные индикаторы компрометации после установки исправлений, и если индикаторы обнаружены, связаться с CISA, чтобы начать действия по реагированию на инциденты. Директива является ответом на наблюдаемое активное использование этих продуктов с использованием ранее неизвестных уязвимостей. CISA также выпустила оповещение об активности для предоставления дополнительной информации и поощрения других организаций государственного и частного секторов к принятию мер по защите своих сетей.

«Эта чрезвычайная директива поможет нам защитить федеральные сети от непосредственной угрозы, в то время как CISA будет работать со своими межведомственными партнерами, чтобы лучше понять методы и мотивы злоумышленника, чтобы поделиться ими с нашими заинтересованными сторонами», - сказал исполняющий обязанности директора CISA Брэндон Уэльс. «Скорость, с которой CISA выпустила эту Директиву о чрезвычайной ситуации, отражает серьезность этой уязвимости и важность того, чтобы все организации - в правительстве и частном секторе - предприняли шаги по ее устранению».

ED 21-02 отражает решение CISA о том, что эксплуатации, представляющие неприемлемый риск для федеральных гражданских органов исполнительной власти, требуют принятия срочных мер. Компания CISA сделала эту оценку на основании 1) текущего использования этих уязвимостей, 2) вероятности широкого использования уязвимостей после публичного раскрытия информации и риска того, что услуги федерального правительства американскому населению могут быть снижены.

CISA и Агентство национальной безопасности работали с Microsoft и исследователями безопасности, чтобы определить подходы к обнаружению и смягчению этих уязвимостей, для которых Microsoft выпустила исправление сегодня днем. Облачные сервисы, такие как системы Microsoft 365 и Azure, не подвержены этой уязвимости». ***(CISA ISSUES EMERGENCY DIRECTIVE REQUIRING FEDERAL AGENCIES TO PATCH CRITICAL VULNERABILITY // Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/news/2021/03/02/cisa-issues-ed-requiring-federal-agencies-patch-critical-vulnerability). 03.03.2021).***

***

«Масштабы взлома Microsoft Exchange начинают проявляться, когда десятки тысяч организаций потенциально скомпрометированы.

Атака использовала ранее неизвестные недостатки в программном обеспечении электронной почты, а иногда и украденные пароли, чтобы украсть данные из сетей целей.

Microsoft заявляет, что злоумышленники «спонсируются государством и действуют за пределами Китая».

И хотя изначально компания думала, что количество атак было «ограниченным», с тех пор она сообщила о «более широком использовании» этой тактики - вероятно, потому, что другие хакеры собираются, чтобы воспользоваться теперь общедоступными уязвимостями до того, как системы будут исправлены.

Под давлением

Все это происходит сразу после кибер-кампании SolarWinds, связанной с Россией, которая затронула несколько правительственных ведомств США и другие организации.

На этот раз компании и другие затронутые организации, по-видимому, имеют меньшее стратегическое значение.

Но даже в этом случае эти две атаки вынудили новую администрацию Байдена отреагировать.

А уставшие киберзащитники говорят, что события не просто нарастают, а выходят из-под контроля.

И Россия, и Китай отрицают свою причастность.

Жесткий разговор

Советник по национальной безопасности США Джейк Салливан написал в Твиттере, что Белый дом «внимательно отслеживает» сообщения о последнем взломе, что является признаком того, что администрация хочет, чтобы ее рассматривали серьезно.

Один сенатор США охарактеризовал атаку SolarWinds как «акт войны».

Другие не согласились.

Но это показывает, как усиливается риторика о кибер-кампаниях, усиливая давление для принятия жестких мер.

Хотя неясно, какие действенные варианты есть у президента.

И есть опасения, что его администрация жестко заговорила о себе, когда неясно, действительно ли она может сдерживать противников.

New York Times сообщила, что официальные лица США заявили, что "первым шагом" в "ближайшие недели" станет серия тайных акций в российских сетях.

Скорее всего, они будут сопровождаться экономическими санкциями и какой-то публичной атрибуцией.

Телеграфирование планов тайных атак может показаться немного странным.

Но отчасти дело в ответе…

Со своей стороны, Великобритания готовится начать собственный обзор безопасности и обороны, в котором, как ожидается, будет участвовать Китай.

Он сказал меньше, чем США о последнем взломе, хотя он исследует его влияние.

Остановка операций

Киберкомандование вооруженных сил США в последние годы придерживалось стратегии «защищаться вперед» и «настойчиво сражаться».

Это означает взлом систем противника, чтобы выяснить, что они делают, и прекращение операций против США до того, как они будут прекращены.

В преддверии промежуточных выборов 2018 года военные операторы США получили доступ к системам российских операторов, рассылающих пропагандистские материалы, направленные на выборы.

Сообщается, что они заблокировали доступ в Интернет и отправили сообщения, в которых говорилось, что США знают, чем они занимаются.

Это противостояние киберпространству многие сочли назревшим.

Но Россия и Китай, похоже, это не испугали.

Один из вариантов сейчас - нанести более сильный ответный удар.

Но эскалация связана с риском.

Критики обеспокоены тем, что атаке по-прежнему уделяется больше внимания и ресурсов, чем защите.

Кража информации

Недавние события также высветили проблемы в стратегии США по установлению «норм» в киберпространстве.

США сочли шпионаж - кражу информации - приемлемым, потому что они широко практиковали его, как сообщил информатор Эдвард Сноуден в 2013 году.

Проблема Вашингтона в том, что недавние нарушения могут подпадать под ту же категорию.

Это ставит США в затруднительное положение.

И он, кажется, переосмысливает свои собственные красные линии, чтобы сказать, что такие действия на самом деле требуют ответа.

Но только потому, что США устанавливают особую красную черту, нет причин, по которым другие должны ее уважать.

Другие страны часто указывают на тот факт, что США заявляют, что разрушительные кибератаки недопустимы, но были первыми, кто пересек эту черту десять лет назад, когда они использовали атаку Stuxnet для уничтожения частей ядерной системы Ирана.

Нажми сильнее

Все это отражает давнюю напряженность в отношении кибербезопасности США.

Он всегда знал о киберпространстве больше, чем кто-либо другой - отчасти потому, что он в значительной степени его построил.

Это означало, что он мог воспользоваться этим способом, которым могли немногие другие, в том числе для шпионажа.

Но он понял, что он также более уязвим, чем кто-либо другой, потому что он был самым передовым и имел цифровую связь.

В течение многих лет преимущества перевешивали риски.

Но теперь другие страны доказывают, что не только могут, но и готовы действовать еще сильнее и использовать цифровые зависимости.

И это заставило американских политиков ломать голову над тем, как отреагировать». ***(Gordon Corera. Microsoft email server hacks put Biden in a bind // BBC (https://www.bbc.com/news/technology-56325784). 08.03.2021).***

***

«По мнению официальных лиц, более 3000 британских почтовых серверов по-прежнему находятся под угрозой из-за глобальной ошибки электронной почты Microsoft Exchange.

Национальный центр кибербезопасности заявил, что, по оценкам, 7000 серверов были затронуты уязвимостью в Великобритании, и только половина из них была защищена.

Вредоносное ПО было обнаружено на 2300 машинах, но предприятиям помогли удалить его.

Агентство заявило, что «жизненно важно», чтобы все затронутые предприятия приняли меры для защиты своих почтовых серверов.

Объявление раскрывает масштабы проблемы среди британских компаний впервые после того, как возникла проблема глобальной безопасности.

NCSC предупредил, что группы программ-вымогателей начали использовать эту уязвимость для установки своих вредоносных программ, хотя до сих пор не было никаких доказательств широко распространенных атак программ-вымогателей на британские компании.

После установки вымогатель блокирует данные пользователя надежным шифрованием, делая компьютерную систему непригодной для использования. Затем группа требует оплаты, чтобы разблокировать ее, и, если требования не будут выполнены, украдет или удалит данные.

Бесплатно для всех

Недостаток безопасности затрагивает широко используемую систему электронной почты Exchange Microsoft, которая поддерживает электронную почту крупных корпораций, малых предприятий и государственных органов по всему миру.

NCSC особенно обеспокоен малым и средним бизнесом, который, возможно, не слышал об этой проблеме.

Первоначально уязвимость использовалась хакерской группой для получения удаленного доступа к почтовым серверам, с которых она могла украсть конфиденциальные данные.

Но после того, как Microsoft предупредила мир, что она определила проблему, и призвала всех своих пользователей загрузить последние обновления безопасности, другие хакерские группы быстро ознакомились с недостатком.

Результат является широко распространенным и «бесплатным для всех», в то время как большинство хакерских групп пытаются найти незащищенные почтовые серверы для атаки.

«Мы тесно сотрудничаем с отраслью и международными партнерами, чтобы понять масштабы и влияние воздействия на Великобританию, но жизненно важно, чтобы все организации предприняли немедленные шаги для защиты своих сетей», - предупредил директор NCSC по операциям Пол Чичестер.

«Пока эта работа продолжается, самым важным действием является установка последних обновлений Microsoft».

Он также призвал все организации «ознакомиться» с инструкциями по атакам программ-вымогателей и искать любые признаки того, что их системы уже взломаны.

Истинный масштаб этой проблемы все еще проявляется, учитывая, что тысячи систем уязвимы только в Великобритании.

Хотя многие системы по-прежнему подвержены риску и в тысячах установлено вредоносное ПО, количество случаев, когда мы знаем, что оно действительно использовалось для кражи электронных писем или блокировки людей с помощью программ-вымогателей, все еще довольно мало.

Это может измениться в ближайшие дни по мере поступления новых отчетов.

Ясно то, что несколько хакерских групп объединились для эксплуатации уязвимости, и те, кто работает над защитой, вероятно, еще какое-то время будут заняты». ***(Microsoft hack: 3,000 UK email servers remain unsecured // BBC (https://www.bbc.com/news/technology-56372188). 13.03.2021).***

***

«Белый дом усиливает координацию с частным сектором, чтобы устранить продолжительные последствия серьезного взлома программного обеспечения Microsoft, в результате которого тысячи американских организаций оказались уязвимыми для хакеров.

Это включает в себя впервые участие частных компаний в заседаниях межведомственной рабочей группы, посвященной инциденту, сообщил журналистам высокопоставленный представитель администрации.

Это важный шаг на пути к прозрачности для администрации Байдена, которая делает упор на укрепление отношений между частным и государственным сектором в результате хакерской кампании в России SolarWinds, которая проникла как минимум в 9 государственных учреждений и около 100 компаний.

Недавний взлом Microsoft добавил срочности в исправлении этих решений. Ранее Microsoft объявила, что группа хакеров, связанных с Китаем, воспользовалась уязвимостью в ее продукте Microsoft Exchange. С тех пор другие киберпреступники начали использовать серверы, которые еще не были обновлены для устранения уязвимости.

Ситуация обострилась, когда Microsoft сообщила, что хакеры нацелены на уязвимые серверы с помощью программы-вымогателя, программного обеспечения, на котором установлена программа, позволяющая хакерам блокировать компьютерные системы и данные за деньги. К уязвимым пользователям Microsoft относятся сотни банков, медицинских и государственных серверов, как выяснили исследователи из фирмы RiskIQ, занимающейся кибербезопасностью. Успешная атака программ-вымогателей против любого из них может создать серьезный хаос.

По словам чиновника, команда Белого дома изучает, как снять озадаченность частного сектора по поводу обмена информацией с правительством. Конгресс также планирует выдвинуть предложения относительно обмена инцидентами в области кибербезопасности в ближайшие недели.

Белый дом также готовит множество предложений по усилению кибербезопасности.

…администрация Байдена взвешивает ряд потенциальных решений, в том числе рейтинговую систему для программного обеспечения. Система выставления оценок будет аналогична той, которая используется местными департаментами здравоохранения для ресторанов. Идея рейтинга кибербезопасности была продвинута двухпартийной Комиссией Конгресса по киберпространству, а также некоторыми отраслевыми группами.

Администрация также обдумывает закон, подобный принятому в Сингапуре, требующий, чтобы домашние устройства были снабжены наклейками безопасности.

По словам высокопоставленного чиновника, в ближайшее время будут приняты административные указы, касающиеся этих двух идей.

Администрация не рассматривает предоставление правительству дополнительных полномочий по слежению за внутренним интернет-трафиком на предмет хакеров. Некоторые эксперты и законодатели обеспокоены тем, что слепое пятно, созданное ограниченными властями, создало для международных хакеров простой способ избежать обнаружения с помощью сетей США. Официальный представитель Байдена сказал, что правительство не рассматривает возможности расширения внутреннего наблюдения, чтобы облегчить американской разведке контроль внутреннего трафика для хакеров, предложение, которое, вероятно, вызовет протесты со стороны защитников конфиденциальности и в Конгрессе.

Предстоящие меры принимаются по мере того, как Белый дом продвигает свое расследование SolarWinds.

…девять агентств, взломанных российскими хакерами, находятся на третьей неделе четырехнедельной программы очистки. Анализ обстоятельств, приведших к атаке, выявил «значительные пробелы в модернизации и технологиях кибербезопасности в федеральном правительстве», - сказал чиновник.

Администрация намеревается отреагировать новой инициативой, которая будет включать внедрение новых технологий для федеральных агентств…

Недавний пакет помощи в связи с коронавирусом включал 650 миллионов долларов для Агентства по кибербезопасности и безопасности инфраструктуры для улучшения защиты от кибербезопасности. До четверти этих денег может пойти осажденной Microsoft для защиты облачных систем федеральных агентств, сообщают Джозеф Менн, Кристофер Бинг и Рафаэль Саттер из Reuters. Планы расходов разозлили некоторых законодателей, которые заявили, что правительство не должно вознаграждать компанию за два недавних взлома.

«Если единственное решение серьезной проблемы, в которой хакеры воспользовались недостатком дизайна, который давно игнорируется Microsoft, - это дать Microsoft больше денег, правительству необходимо пересмотреть свою зависимость от Microsoft», - сказал Рейтер сенатор Рон Уайден.

Ключи

Большое жюри предъявило обвинение двум руководителям компаний, работающим с зашифрованными чатами, в наживании на своих клиентах-преступниках.

Министерство юстиции заявило, что двое канадских мужчин, Жан-Франсуа Ип и Томас Хердман, обвиняются в совершении заговора с целью вымогательства для распространения запрещенных наркотиков с помощью их компании-разработчика зашифрованных приложений Sky. Джозеф Кокс из Motherboard сообщает, что это всего лишь второй раз, когда правительство США выдвинуло обвинения против компании по передаче зашифрованных сообщений.

В обвинительном заключении говорилось, что люди, которые руководили компанией и распространяли зашифрованные устройства, способствовали незаконной деятельности своих пользователей и сговорились с целью оказания помощи и подстрекательства к незаконному распространению кокаина…

Обвинение было предъявлено через несколько дней после того, как европейская полиция арестовала десятки пользователей приложения, которое пользовалось популярностью среди преступников, координировавших свою деятельность. Власти заявляют, что они отслеживали зашифрованные коммуникации приложений за месяц до рейдов и смогли собрать информацию о более чем 100 «запланированных крупномасштабных преступных операциях».

Швейцарская полиция провела обыск в доме хакера, который получил доступ к сотням тысяч изображений с камер наблюдения.

В квартире Тилли Коттманн в Люцерне был проведен обыск в связи с расследованием ФБР по факту взлома и утечки конфиденциальной информации от Mercedes-Benz, Intel и других компаний… Рейд произошел всего через несколько дней после того, как Коттманн заявил, что их хакерский коллектив провел не имеющий отношения к делу взлом, взломав компанию Verkada, производящую камеры наблюдения.

Австралия, Индия, Япония и США договорились сформировать рабочую группу по кибербезопасности.

Создание рабочей группы по кибербезопасности происходит в то время, когда администрация Байдена пытается укрепить свое сотрудничество в области кибербезопасности с союзниками, на котором она сосредоточила свое внимание как на элементе глобальной дипломатии.

«Толчком к созданию этой новой Cyber Working Group стал не только инцидент с SolarWinds или инцидент с Microsoft Exchange, на оба из которых США срочно реагируют, но и кибератаки, которые поразили Японию, Индию и Австралию всего за последние несколько недель и месяцев», - сказал советник по национальной безопасности Джейк Салливан…

Отраслевой отчет

Представитель Google сказал, что Microsoft раскритиковала компанию, чтобы отвлечься от взлома программного обеспечения Microsoft.

Старший вице-президент Google по глобальным связям Кент Уокер обвинил Microsoft в «неприкрытом корпоративном оппортунизме» и сказал, что «не случайно» компания нападает на Google из-за того, как он относится к онлайн-новостям, поскольку он управляет последствиями разрушительного взлома. Microsoft и Google отказались от комментариев, хотя президент Microsoft Брэд Смит подробно обсудил Google на слушаниях в Конгрессе в пятницу». ***(Tonya Riley. The Cybersecurity 202: White House weighs new cybersecurity proposals after two major hacking campaigns // The Washington Post (https://www.washingtonpost.com/politics/2021/03/15/cybersecurity-202-white-house-weighs-new-cybersecurity-proposals-after-two-major-hacking-campaigns/). 15.03.2021).***

***

«Парламент Норвегии присоединился к растущему списку организаций, уязвимых для Microsoft Exchange Server.

Пресс - релиз подтвердил, что Stortinget (большая сборка) пострадал от рук бэкдор-установки злоумышленников и, что еще хуже, «мы знаем, что данные были извлечены, но пока мы не имеем полное представления о ситуации» отметила директор Марианна Андреассен.

«Мы предприняли масштабные действия и не можем исключить, что будут предприняты дальнейшие действия, - добавила она, - работа ведется в сотрудничестве с органами безопасности. Ситуация неясна, и мы не знаем полного потенциала нанесения ущерба. "

Подвиг в демократическом учреждении, таком как Стортинг, безусловно, зловещий, возможно, даже больше, чем беды последних дней таких организаций, как Европейское банковское управление. Президент Stortinget Тон Вильгельмсен Трён сказал: «Атака, с которой мы столкнулись, показывает, что ИТ-атаки могут иметь серьезные последствия для демократических процессов в худшем случае».

Расположенный в Осло Стортинг является высшим законодательным органом Норвегии и состоит из 169 мест. Трёэн является ее президентом с 2018 года.

Сборке не привыкать IT-атаки. Его почтовые системы были взломаны в августе 2020 года, в чем тогда министр иностранных дел Ине Эриксен Сёрейде обвинила Россию. Обвинение было признано "необоснованным" главой комитета Совета Федерации по международным делам Константином Косачевым, сообщает Российское информационное агентство ТАСС.

Стортинг не связывает это нарушение с недавней эксплуатацией уязвимостей в Microsoft Exchange Server, обнародованной на прошлой неделе.

Исследователь безопасности Брайан Кребс недавно сообщил, что «по крайней мере» 30 000 американских организаций могли быть взломаны из-за недостатков, которые позволяли хакерам оставлять бэкдоры на открытых серверах Exchange. 2 марта Microsoft выпустила экстренные обновления и заявила, что в атаках виновата группа хакеров, поддерживаемых Пекином.

Кребс подсчитал, что группа «засеяла сотни тысяч организаций-жертв по всему миру инструментами, которые дают злоумышленникам полный удаленный контроль над пораженными системами».

Отчасти проблема заключается в том, что внимание, привлеченное к недостаткам, привело к потоку атак злоумышленников, стремящихся скомпрометировать системы, прежде чем жертвы смогут применить необходимые исправления. Джон Халтквист, вице-президент Mandiant Threat Intelligence, заявил вчера: «По мере того, как эти эксплойты будут распространяться среди преступных элементов, эта проблема станет кризисом для организаций с минимальными ресурсами.

Что действительно является частью проблемы. Администрирование Exchange Server - нетривиальное дело, и установка исправлений и сканирование на предмет компрометации не для слабонервных (а также то, почему Европейское банковское управление отключило свои серверы из Интернета при первых признаках проблемы).

К сожалению, Stortinget вряд ли станет последней организацией, которая станет публичной из-за компрометации Microsoft Exchange». ***(Richard Speed. Å nei! Norway's Stortinget struck by Microsoft Exchange malware // The Register (https://www.theregister.com/2021/03/11/stortinget_attack/). 11.03.2021).***

***

«Microsoft сообщает, что 92% серверов Exchange, уязвимых для ряда критических уязвимостей, теперь исправлены или приняты меры по их устранению.

Команда Security Response гиганта из Редмонда заявила, что «набирает обороты» патчи или инструменты смягчения последствий, применяемые к локальным серверам, выходящим в Интернет, и последние данные показывают улучшение на 43% по всему миру по сравнению с прошлой неделей.

Microsoft процитировала телеметрию от RiskIQ, который работает с технологическим гигантом над устранением последствий инцидента безопасности, в твите, опубликованном в понедельник.

2 марта Microsoft выпустила экстренные исправления для Microsoft Exchange Server 2013, Exchange Server 2016 и Exchange Server 2019. В то время компания

заявила, что четыре уязвимости нулевого дня, которые могут привести к краже данных и общему захвату сервера, активно используются в «ограниченные, целевые атаки».

Однако вскоре несколько групп расширенных постоянных угроз (APT) начали присоединяться к кампаниям на базе Exchange Server, и, по оценкам, тысячи систем, принадлежащих организациям по всему миру, были скомпрометированы.

Наряду с аварийными исправлениями Microsoft также опубликовала руководство по смягчению последствий и создала инструмент устранения последствий в один клик, включая перезапись URL-адреса для одной из уязвимостей, чтобы остановить формирование цепочки атак.

Кроме того, был обновлен антивирус Microsoft Defender Antivirus, в который включены функции автоматического устранения уязвимостей нулевого дня.

Однако проблема с этими уязвимостями заключается в том, что применение патча или средств защиты не удаляет существующие инфекции. F-Secure заявляет, что «десятки тысяч» серверов уже взломаны, а другие «[взламываются] быстрее, чем мы можем сосчитать».

Несмотря на то, что исправления и меры по снижению рисков применяются с большой скоростью, ИТ-администраторы должны проверять свои системы на наличие индикаторов компрометации (IoC) и выполнять аудит безопасности, чтобы увидеть, не использовались ли их серверы до применения обновлений безопасности». ***(Charlie Osborne. Microsoft: 92% of vulnerable Exchange servers are now patched, mitigated // ZDNet (https://www.zdnet.com/article/microsoft-92-of-vulnerable-exchange-servers-are-now-patched-mitigated/). 24.03.2021).***

***

«Недавно исправленные уязвимости в Microsoft Exchange вызвали новый интерес у киберпреступников, которые увеличили количество атак, сосредоточенных на этом конкретном векторе.

В то время как количество атак программ-вымогателей увеличилось за последние шесть месяцев, компания Check Point, занимающаяся кибербезопасностью, на прошлой неделе заметила всплеск инцидентов, нацеленных на серверы Microsoft Exchange, уязвимые для так называемых критических ошибок ProxyLogon.

Даже несмотря на то, что установка исправлений идет быстрыми темпами, компания отметила, что количество попыток атак по всему миру утроилось, насчитывая десятки тысяч.

Microsoft Exchange по-прежнему привлекателен

По данным Microsoft, 14 марта было около 82 000 уязвимых серверов Exchange. Примерно через неделю это число значительно упало до примерно 30 000 уязвимых машин, согласно данным RiskIQ.

Данные телеметрии от Check Point на прошлой неделе показали, что во всем мире было совершено более 50 000 попыток атак, большинство из которых были нацелены на организации в правительственном / военном, производственном и банковском / финансовом секторах.

Почти половина попыток использования эксплойтов произошла в США (49%), что на сегодняшний день является наиболее привлекательным регионом по сравнению с другими странами, где Check Point зарегистрировал гораздо меньше инцидентов (Великобритания - 5%, Нидерланды и Германия - по 4%).

Атаки программ-вымогателей растут, WannaCry все еще остается проблемой

Компания зафиксировала рост атак программ-вымогателей на 57% за последние шесть месяцев на глобальном уровне. Более тревожным является постоянный ежемесячный рост на 9% с начала года.

Помимо наблюдаемых обычных штаммов вымогателей (Maze, Ryuk, REvil), компания отмечает рост на 53% числа организаций, пострадавших от вируса-вымогателя WannaCry.

Почти четыре года назад эпидемия WannaCry распространилась через блок сообщений NSA EternalBlue для Windows Server Message Block (SMB), в результате чего всего за несколько дней был нанесен ущерб в сотни миллионов долларов США.

Его распространение было приостановлено после того, как исследователь безопасности Маркус Хатчинс обнаружил аварийный выключатель и Microsoft выпустила исправления. Атакам подверглись более 200 000 компьютеров.

Однако вредоносное ПО не было уничтожено. Охранные фирмы продолжают обнаруживать WannaCry даже в наши дни. В январе это было крупнейшее обнаружение программ-вымогателей TrendMicro.

Причина такого большого числа в том, что WannaCry подвержен заражению червями, а тысячи систем по-прежнему уязвимы для EternalBlue и доступны через общедоступный Интернет.

Check Point наблюдала ту же тенденцию, начиная с декабря 2020 года, и в марте 2021 года количество атак продолжало увеличиваться более чем на 12000.

Цифры показывают важность своевременной установки исправлений, в противном случае организации остаются уязвимыми для векторов атак, которые в большинстве случаев должны исчезнуть». ***(Ionut Ilascu. Microsoft Exchange attacks increase while WannaCry gets a restart // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/microsoft-exchange-attacks-increase-while-wannacry-gets-a-restart/). 30.03.2021).***

***

Технічні аспекти кібербезпеки

«Исследователи обнаружили, что большинству агентств безопасности не удается должным образом дезинфицировать файлы в формате Portable Document Format (PDF) перед их публикацией, тем самым раскрывая потенциально конфиденциальную информацию и открывая двери для атак.

По словам Суприя Адхатарао и Седрика Лораду, двух исследователей из Университета Гренобль-Альпы и Национального института Франции. Исследования в области компьютерных наук и автоматизации (Inria), анализ примерно 40 000 PDF-файлов, опубликованных 75 службами безопасности в 47

странах, показал, что эти файлы могут использоваться для идентификации сотрудников, использующих устаревшее программное обеспечение.

Анализ также показал, что использование такой обработки в агентствах безопасности довольно низкое, поскольку только 7 из них использовали ее для удаления скрытой конфиденциальной информации из некоторых опубликованных PDF-файлов. Более того, 65% очищенных файлов по-прежнему содержали скрытые данные.

«Некоторые агентства используют слабые методы очистки: для этого требуется удалить всю скрытую конфиденциальную информацию из файла, а не просто удалить данные с «поверхности». Органы безопасности должны изменить свои методы «санитарной» обработки», - говорят исследователи.

Файлы PDF, как отмечают исследователи, представляют собой коллекции косвенных объектов (восемь типов объектов: массивы, логические значения, словари, имена, числа, потоки, строки и нулевой объект), которые используются для хранения данных. Эти объекты могут включать скрытые данные, невидимые при просмотре PDF.

Согласно NSA, в файлах PDF есть 11 основных типов скрытых данных, а именно метаданные; встроенный контент и прикрепленные файлы; скрипты; скрытые слои; встроенный поисковый индекс; хранимые данные интерактивной формы; просмотр и комментирование; скрытая страница, изображение и данные обновления; скрытый текст и изображения; комментарии PDF, которые не отображаются; и данные без ссылок.

Метаданные, связанные с изображениями в файле PDF, могут использоваться для сбора информации об авторе, так же как комментарии и аннотации, которые не были удалены перед публикацией, и метаданные PDF.

Существует несколько инструментов, которые можно использовать для очистки файлов PDF, включая Adobe Acrobat; также существует четыре уровня очистки: Уровень 0: полные метаданные (без очистки), Уровень 1: частичные метаданные, Уровень 2: без метаданных, и Уровень-3: правильно очищенные файлы (полная очистка, все объекты удалены).

Для своего исследования ученые использовали набор из 39 664 PDF-файлов. Из них 1783 (4%) содержали имя автора, 30 155 (76%) содержали метаданные об инструменте производителя PDF, а 16 805 (42%) указывали на используемую операционную систему.

Из файлов также просочились адреса электронной почты, в их числе, официальные (в 52 файлах), марки оборудования (581 файл) и пути (1814 PDF-файлов).

«В ходе нашего анализа мы заметили, что многие агентства включают более одного автора, публикующего файлы PDF. Можно скачать все PDF-файлы, опубликованные на сайте охранного агентства, и наблюдать за привычками авторов, тенденциями в ОС», - отмечают исследователи.

Анализ также позволил идентифицировать 159 сотрудников в 19 агентствах, которые не обновляли инструменты в течение двух лет, из-за чего они могут быть использованы злоумышленниками в целевых атаках, тем более что почти половина файлов PDF утекла в данные операционной системы.

В то время как 9 509 (24%) проанализированных файлов PDF были обработаны перед публикацией, только 3 313 (8%) были обработаны с помощью Уровня-3. Исследователи отмечают, что только 3 агентства из 7, которые, похоже, заботятся о обработке, делают это должным образом.

«Проблема в том, что популярные инструменты для создания PDF-файлов по умолчанию сохраняют метаданные вместе со многими другими данными при создании PDF-файла. Они не предоставляют возможности для очистки, или это может быть достигнуто только путем выполнения сложной процедуры. Программное обеспечение, создающее файлы PDF, по умолчанию требует принудительной очистки. Пользователь должен иметь возможность добавлять метаданные только в качестве опции», - заключают ученые». ***(Ionut Arghire. Research: Security Agencies Expose Information via Improperly Sanitized PDFs // Wired Business Media (https://www.securityweek.com/research-security-agencies-expose-information-improperly-sanitized-pdfs?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Securityweek+%28SecurityWeek+RSS+Feed%29). 15.03.2021).***

***

«Google выпустил код подтверждения концепции (PoC), чтобы продемонстрировать практичность атак Spectre по побочному каналу против движка JavaScript браузера для утечки информации из его памяти…

Веб-разработчики могут посетить новую страницу Google - https://leaky.page - чтобы увидеть демонстрацию Spectre на JavaScript, видео-демонстрацию на YouTube и подробное описание PoC на GitHub.

Google выпустил PoC для разработчиков веб-приложений, чтобы понять, почему важно развертывать средства защиты на уровне приложений. На высоком уровне, как подробно описано в документе Google по W3C, «данные разработчика не должны неожиданно попасть в процесс злоумышленника».

Хотя PoC демонстрирует атаку JavaScript Spectre против движка JavaScript V8 Chrome 88 на процессоре Intel Core i7-6500U «Skylake» в Linux, Google отмечает, что его можно легко настроить для других процессоров, версий браузеров и операционных систем. Он был успешным даже на процессоре Apple M1 Arm с небольшими изменениями. Атака может привести к утечке данных со скоростью 1 КБ в секунду.

Основными компонентами PoC являются «гаджет» Spectre версии 1 или код, запускающий контролируемое злоумышленником временное выполнение; и побочный канал или «способ наблюдать побочные эффекты временного выполнения».

«Веб-платформа полагается на происхождение как на фундаментальную границу безопасности, и браузеры неплохо справляются с задачей предотвращения явной утечки данных из одного источника в другой», - пояснил Майк Уэст из Google.

«Атака, как Спектр, однако, показать, что у нас еще есть работа, чтобы сделать, чтобы смягчить неявную утечку данных. Побочные каналы эксплуатируемых через эти атаки доказывают, что злоумышленники могут читать

любые данные, поступающие в процесс хостинга, что код нападавшего. Эти атаки довольно практичны сегодня и представляют реальную опасность для пользователей».

Хотя Google и другие поставщики браузеров разработали средства защиты Spectre, такие как Site Isolation, они не предотвращают использование Spectre, объясняют Стивен Рёттгер и Артур Янк, инженеры по информационной безопасности Google.

«Скорее [эти меры] защищают конфиденциальные данные от присутствия в тех частях памяти, из которых они могут быть прочитаны злоумышленником», - отмечают они в блоге…

Google также выпустил новый прототип расширения Chrome под названием Spectroscope, которое сканирует приложение, чтобы найти ресурсы, которые могут потребовать включения дополнительных средств защиты.

Рёттгер и Янк отмечают, что гаджет Варианта 1 можно смягчить на программном уровне. Однако команда V8 обнаружила, что смягчение последствий Spectre Variant 4 или Speculative Store Bypass (SSB) «просто невозможно программно». ***(Liam Tung. Google: This Spectre proof-of-concept shows how dangerous these attacks can be // ZDNet (https://www.zdnet.com/article/google-this-spectre-proof-of-concept-shows-how-dangerous-these-attacks-can-be/). 15.03.2021).***

***

«Специалисты по перебору микросхем в Америке изобрели еще один способ похитить конфиденциальные данные, используя выбор конструкции процессоров Intel.

Докторант Риккардо Пакканелла, магистрант Личенг Луо и доцент Кристофер Флетчер из Университета Иллинойса в Урбана-Шампейн изучили, как работают межкомпонентные соединения с кольцом ЦП, и обнаружили, что их можно использовать для атак по побочным каналам. В результате одно приложение может определять частную память другого приложения и отслеживать нажатия клавиш пользователем.

«Это первая атака, использующая конкуренцию за межъядерное соединение процессоров Intel», - сказал Пакканелла The Register. «Атака не полагается на совместное использование памяти, наборов кешей, частных ресурсов ядра или каких-либо конкретных структур uncore. Как следствие, ее трудно смягчить с помощью существующей защиты побочного канала».

Атаки по побочным каналам, такие как уязвимости Spectre и Meltdown 2018 года, используют характеристики современной микроархитектуры микросхемы для раскрытия или вывода секретов посредством взаимодействия с общим вычислительным компонентом или ресурсом.

В документе [PDF], который будет представлен на выставке USENIX Security 2021 в августе - «Властелин кольца (a): атаки по побочным каналам на межкомпонентное кольцевое соединение ЦП практически осуществимы» - Пакканелла, Луо и Флетчер рассказывают, как им удалось чтобы выяснить, как работает кольцевое соединение Intel, или шина, по которой информация передается между ядрами ЦП.

Вооруженные этим пониманием, они обнаружили, что могут утечь биты криптографического ключа из реализаций RSA и EdDSA, которые уже известны как уязвимые для атак по побочным каналам. Они также показали, что могут отслеживать время нажатия клавиш, что, как показали предыдущие исследования, можно использовать для восстановления введенных паролей.

Копаемся в Роковой горе

Перед исследователями стояла двоякая задача: во-первых, Intel не предоставила подробностей о том, как работает кольцевая шина процессора. Требовался столь серьезный реверс-инжиниринг.

Во-вторых, их атака основана на конкуренции, которая в данном случае включает мониторинг задержки, когда разные процессы обращаются к памяти одновременно. Такое наблюдение затруднено, потому что есть много шума, который необходимо идентифицировать и отфильтровать, а значимые события, такие как промахи частного кеша (когда система ищет данные в кеше, которого нет), - это еще не все. общий.

«На очень высоком уровне идея состоит в том, что доступ к памяти одного процесса задерживает доступ к памяти другого процесса из-за ограниченной пропускной способности межсоединения общего кольца», - сказал Пакканелла.

«Благодаря знаниям, полученным в результате обратного проектирования, злоумышленник / получатель может настроить себя так, чтобы его нагрузки гарантированно задерживались из-за доступа к памяти жертвы / отправителя, и использовать эти задержки в качестве побочного канала».

По сути, эти повторяющиеся загрузки памяти могут вызывать задержки, раскрывающие секреты наблюдателю.

Пакканелла сказал, что в двух продемонстрированных атаках злоумышленник запускает на компьютере жертвы непривилегированный код - например, вредоносное ПО, скрытое в программной библиотеке или приложении, которое отслеживает другие программы или пользователей. Он сказал, что облачный сценарий, в котором противник является администратором или со-арендатором общей системы, также возможен, но он и его коллеги предпочитают не делать этого утверждения, поскольку демонстрационные атаки проводились в невиртуализированной среде. и не тестировался в других обстоятельствах.

Хорошо, так что немного основ

Криптографическая атака предполагает, что одновременная многопоточность (SMT) отключена, что кэш последнего уровня (LLC) разделен на разделы для защиты от атак на основе многоядерных кешей, а совместное использование памяти между доменами безопасности отключено. Также предполагается, что система настроена на очистку кэш-памяти целевого объекта для предотвращения атак с упреждающим планированием на основе кеша.

Атаки были протестированы на процессорах Intel Coffee Lake и Skylake, процессорах клиентского класса и должны работать на серверных процессорах, таких как Xeon Broadwell. Неизвестно, восприимчивы ли более поздние серверные чипы Intel с межкомпонентными сетями. Точно так же исследователи не рассматривали, как их методика будет работать на процессорах ARM, которые полагаются на другую технологию межсоединений.

Intel, которая вместе с Национальным научным фондом помогла поддержать это исследование, не слишком обеспокоена вмешательством шины ЦП.

«Intel классифицировала нашу атаку как «традиционный побочный канал» (например, TLBleed, Портсмаш и т. Д.), - сказал Пакканелла. «Они относятся к этому классу атак иначе, чем к классу «атак со спекулятивным исполнением / временным исполнением» (например, Spectre, Meltdown и т. Д.). То есть они не рассматривают традиционные атаки по побочным каналам как значительную ценность для злоумышленника, и они уже опубликовали предлагаемые ими рекомендации о том, как смягчить их в программном обеспечении здесь и здесь ".

Частично совет Intel предполагает использование принципов программирования с постоянным временем [PDF] в качестве защиты от атак, основанных на времени.

В документе отмечается, что такие меры обеспечат защиту от криптографической атаки, которая зависит от кода, не находящегося в постоянном времени. Но Пакканелла предполагает, что это не данность.

«По-настоящему постоянный код может быть трудно реализовать на практике», - сказал он. «Кроме того, для достижения «изоляции домена» в кольцевом межсоединении потребуется дополнительная аппаратная поддержка».

Исследователи планируют выпустить свой экспериментальный код, как только они сделают свою статью доступной в воскресенье, 7 марта». ***(Thomas Claburn. Intel CPU interconnects can be exploited by malware to leak encryption keys and other info, academic study finds // The Register (https://www.theregister.com/2021/03/08/intel_ring_flaw/). 08.03.2021).***

***

«Исследователи раскрыли больше информации о том, как им удалось взломать несколько веб-сайтов правительства Индии.

В прошлом месяце исследователи из хакерской группы Sakura Samurai частично раскрыли, что они взломали киберсистемы правительства Индии после обнаружения большого количества критических уязвимостей.

Обнародованные сегодня полные результаты проливают свет на используемые исследователями маршруты, включая обнаружение открытых каталогов .git и файлов .env в некоторых из этих систем.

Исследователи обнаруживают открытые файлы .git и .env

В прошлом месяце этичные хакеры Джексон Генри, Роберт Уиллис, Обри Коттл, Джон Джексон и Зултан Холдер совместно работали над поиском уязвимостей, скрывающихся в правительственных системах Индии.

По словам исследователей, разведывательные работы проводились в соответствии с государственной программой раскрытия информации об уязвимостях (RVDP) NCIIPC.

В результате этого командного упражнения исследователи обнаружили ряд серьезных недостатков, в том числе 35 случаев раскрытия пар учетных данных для критически важных приложений, общедоступные конфиденциальные файлы, раскрывающие 13000 записей PII, десятки полицейских отчетов и т. д.

Исследователи также обнаружили уязвимости к перехвату сеанса и удаленному выполнению кода (RCE) в чувствительных государственных системах, обрабатывающих финансовую информацию.

Но вся эта информация стала известна, когда исследователи обнаружили открытые папки .git и файлы .env на одном или нескольких субдоменах правительства Индии.

Во-первых, Генри и Холдер использовали этические хакерские инструменты, чтобы определить целевые поддомены.

Кроме того, они идентифицировали открытые файлы .git и .env на этих серверах, у которых были учетные данные для нескольких приложений, баз данных и серверов.

.Env файл часто используется программными приложениями и содержит информацию о конфигурации вместе с именами пользователей, пароли для серверов и баз данных приложений, таких как MySQL, SMTP, PHPMailer и Wordpress.

Аналогичным образом, каталог .git содержит информацию о кодовой базе программного проекта.

Исследователи использовали инструмент под названием git-dumper для получения содержимого общедоступного. git, и поэтому может получать файлы с именами пользователей и паролями.

Кроме того, Уиллис обнаружил папку / files / на веб-сайте регионального управления полиции с кучей файлов PDF.

Эти PDF-файлы представляли собой полицейские отчеты с конфиденциальной информацией, а некоторые даже содержали данные судебно-медицинской экспертизы.

Многие правительственные ведомства Индии взломали

Продолжив свои разведывательные работы, исследователи продолжили обнаруживать еще больше общедоступных файлов на государственных сайтах, таких как дампы SQL и базы данных, которые должны были оставаться недоступными через Интернет.

Только один пример ниже показывает характер информации, позволяющей установить личность (PII), которая могла быть получена исследователями.

Таблица, показанная ниже, содержит такие поля, как полное имя сотрудника, дата рождения, контактная информация, офисный отдел и номер Aadhar (национального удостоверения личности).

Подтверждая собранную информацию и связывая уязвимости вместе, исследователи могут выполнять атаки с перехватом сеанса и в некоторых случаях удаленное выполнение кода (RCE) против критически важных государственных систем…

После того, как исследователи сообщили о недостатках через посреднические правительственные органы, такие как Национальный координатор по кибербезопасности Индии (NCSC) и CERT-IN, недостатки в конечном итоге были исправлены.

21 февраля 2021 года сотрудник Национального координатора по кибербезопасности (NCSC) генерал-лейтенант Раджеш Пант сказал Hindustan

Times: «Исправительные меры были приняты NCIIPC (Национальный центр защиты критической информационной инфраструктуры) и Cert-IN (Индийская группа реагирования на компьютерные чрезвычайные ситуации)… NCIIPC занимается только критическими проблемами информационной инфраструктуры. В этом случае баланс принадлежал другим штатам и ведомствам, о которых Cert-IN немедленно проинформировал. Вполне вероятно, что некоторые действия могут быть отложены пользователями на уровне штата, который мы проверяем».

Чтобы помешать злоумышленникам использовать эти уязвимости, исследователи до сегодняшнего дня не публиковали полную информацию о том, как именно они использовали правительственные системы.

«После работы с NSCS мы получили зеленый свет на раскрытие более конкретных деталей, и все 34 страницы обнаруженных нами уязвимостей были должным образом устранены», - заявили исследователи в опубликованном сегодня подробном отчете.

Это не первый раз, когда веб-серверы открывают доступ к файлам, которые должны оставаться запрещенными для публики.

Ранее группа Sakura Samurai нарушила требования Организации Объединенных Наций, обнаружив незащищенные файлы учетных данных Git на доменах, принадлежащих ООН.

Исследователи могли использовать эти учетные данные для доступа к более чем 100 000 записей сотрудников ЮНЕП…». ***(Ax Sharma. Researchers hacked Indian govt sites via exposed git and env files // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/researchers-hacked-indian-govt-sites-via-exposed-git-and-env-files/). 12.03.2021).***

***

Виявлені вразливості технічних засобів та програмного забезпечення

«Третий раз в этом году Google представил срочное исправление, чтобы блокировать атаки нулевого дня, поражающие его флагманский браузер Chrome.

Последний аварийный патч для Chrome, доступный для Windows, MacOS и Linux, обеспечивает защиту как минимум от пяти (5) задокументированных уязвимостей. Три из пяти ошибок имеют наивысший рейтинг серьезности Google…

Компания не публиковала никакой дополнительной информации о реальных атаках или платформах операционных систем, на которые они направлены.

Это третья атака нулевого дня, поразившая пользователей Chrome в 2021 году, и во всех трех случаях Google скупился на информацию об используемом вредоносном ПО, платформах ОС или индикаторах компрометации, которые помогли бы защитникам предприятий.

Известей случай, когда государство Северной Кореи взломало исследователей безопасности, Google едва ли подтвердил существование у Chrome

нулевого дня с единственной строчкой, упомянув, что установки Chrome с полностью исправленными исправлениями были скомпрометированы.

Последний «нулевой день» описывается просто как уязвимость в механизме рендеринга Blink Chrome, о которой анонимно сообщили в Google.

Напротив, когда исследовательские группы Google обнаружили масштабную операцию кибершпионажа, свирепствующую на платформе Apple iOS, компания выпустила захватывающий пост в блоге с «очень глубоким погружением в цепочки эксплойтов iOS, которые можно найти в «дикой природе».

Патч для Chrome передается пользователям Chrome через механизм автоматического обновления браузера, но пользователям настоятельно рекомендуется перезапустить сеансы браузера, чтобы правильно применить исправления». ***(Ryan Naraine. Google Chrome Zero-Day Under Attack, Again // Wired Business Media (https://www.securityweek.com/google-chrome-zero-day-under-attack-again). 15.03.2021).***

***

«Одним из преимуществ Linux является то, что он поддерживает очень много старого оборудования. Приложив немного усилий, практически нет вычислительного оборудования, на котором не работает Linux. Это хорошие новости. Плохая новость заключается в том, что иногда в старых программах можно найти древние дыры в безопасности. Так обстоит дело с драйвером передачи данных Linux's Small Computer System Interface (SCSI).

Три дыры в безопасности - CVE-2021-27365, CVE-2021-27363 и CVE-2021-27364 - были обнаружены исследователями компании по безопасности GRIMM в почти забытом углу основного ядра Linux. Первые два из них имеют оценку общей системы оценки уязвимостей (CVSS) выше 7, что является высоким показателем. Хотя у вас, возможно, давно не было диска SCSI или iSCSI, эти 15-летние ошибки все еще существуют. Один из них может быть использован в атаке с повышением локальных привилегий (LPE). Другими словами, обычный пользователь может использовать их, чтобы стать пользователем root…

Правда, уязвимый код SCSI не загружается по умолчанию в большинстве настольных дистрибутивов. Но на серверах Linux все обстоит иначе. Если вашему серверу требуется RDMA (удаленный прямой доступ к памяти), сетевая технология с высокой пропускной способностью и малой задержкой, он, вероятно, автоматически загрузит модуль ядра Linux rdma-core, который несет с собой уязвимый код SCSI.

Использовать дыру непросто, но GRIMM выпустил доказательство концепции эксплойта, в котором показано, как использовать две уязвимости. Теперь, когда путь показан, вы можете рассчитывать на то, что злоумышленники попробуют его.

В частности, уязвимы системы CentOS 8, Red Hat Enterprise Linux (RHEL) 8 и Fedora, где непривилегированные пользователи могут автоматически загружать необходимые модули, если установлен пакет rdma-core. SUSE Linux Enterprise Server (SLES) также может быть атакован. Ubuntu 18.04 и более ранние версии также открыты для атак. И, конечно же, если вы действительно используете диски

SCSI или iSCSI, на вас могут напасть…». ***(Steven J. Vaughan-Nichols. Old Linux storage bugs, new security patches // ZDNet (https://www.zdnet.com/article/old-linux-storage-bugs-new-security-patches/). 15.03.2021).***

***

«Количество хакеров, обнаруживающих уязвимости в системе безопасности и отправляющих их в одну из самых известных программ поощрения ошибок, увеличилось почти на две трети за последний год.

В отчете о хакерах за 2021 год от платформы bug bounty HackerOne подробно рассказывается о развитии тестирования на проникновение и этического взлома за последние 12 месяцев и говорится, что за этот период количество хакеров, отправивших сообщения об уязвимостях, увеличилось на 63 процента.

Целью схем поощрения ошибок является предоставление этичным хакерам средств обнаружения и раскрытия этих уязвимостей до того, как киберпреступники воспользуются ими. Только за последний год хакеры заработали 40 миллионов долларов за раскрытие уязвимостей в программе вознаграждений за ошибки HackerOne по сравнению с 19 миллионами долларов в 2019 году.

В то время как большинство людей, ищущих уязвимости, сосредоточены на веб-приложениях, наблюдается рост числа тех, кто изучает другие потенциальные недостатки, с большим увеличением количества сообщений об уязвимостях, связанных с Android, устройствами Интернета вещей и API-интерфейсами.

В то время как финансовые стимулы для поиска уязвимостей играют определенную роль во взломе - 76 процентов опрошенных HackerOne заявили, что они делают это для заработка, - 85 процентов тех, кто участвует в схемах вознаграждения за ошибки, говорят, что они участвуют, чтобы учиться, а двое третьи делают это для развлечения…». ***(Danny Palmer. Bug bounties: More hackers are spotting vulnerabilities across web, mobile and IoT // ZDNet (https://www.zdnet.com/article/bug-bounties-more-hackers-are-spotting-vulnerabilities-across-web-mobile-and-iot/). 09.03.2021).***

***

«Команда хакеров iPhone выпустила новый инструмент для взлома почти каждого iPhone, включая самые последние модели, используя ту же уязвимость, которая, как сообщила Apple в прошлом месяце, подверглась активным атакам хакеров.

Команда Unc0ver выпустила свой последний джейлбрейк на этих выходных и заявляет, что он работает с iOS 11 (iPhone 5s и новее) до iOS 14.3, которую Apple выпустила в декабре.

Джейлбрейк - это игра в кошки-мышки между исследователями безопасности, которые хотят большего контроля и настройки своих телефонов, и Apple, которая заявляет, что блокирует iPhone в целях безопасности. Хакеры создают инструменты для взлома, находя и используя уязвимости, которые могут снять некоторые из ограничений, которые вводит Apple, например, установка приложений за пределами своего магазина приложений, к которым уже привыкло большинство пользователей Android.

В своем твите группа взломщиков заявила, что использовала «собственный эксплойт» для CVE-2021-1782, уязвимости ядра, которая, по словам Apple, была одной из трех уязвимостей, которые «могли активно использоваться» хакерами. Нацеливаясь на ядро, хакеры могут глубоко проникнуть в базовую операционную систему.

Apple исправила уязвимость в iOS 14.4, выпущенной в прошлом месяце, которая также препятствует работе джейлбрейка в более поздних версиях. Признание того, что iPhone подвергался активной атаке хакеров, было редкостью, но компания отказалась сообщить, кто были эти хакеры и на кого они нацелены. Apple также предоставила анонимность исследователю, сообщившему об ошибке.

Последний джейлбрейк группы, который поддерживал iPhone под управлением iOS 11 - iOS 13.5, был исправлен за считанные дни в прошлом году. Apple работает быстро, чтобы понять и исправить уязвимости, обнаруженные группами взлома, поскольку те же самые уязвимости могут быть использованы злонамеренно.

Эксперты по безопасности обычно советуют пользователям iPhone не делать взлом, поскольку это делает устройство более уязвимым для атак. И хотя поддержание вашего телефона в актуальном состоянии может включать исправления безопасности, которые удаляют джейлбрейк, это один из лучших способов обеспечить безопасность вашего устройства». ***(Zack Whittaker. Hackers release a new jailbreak tool for almost every iPhone // TechCrunch (https://techcrunch.com/2021/03/01/hackers-unc0ver-jailbreak-iphone/). 01.03.2021).***

***

«Уязвимость системы безопасности Cisco существует в маршрутизаторах RV132W ADSL2 + Wireless-N VPN и маршрутизаторах RV134W VDSL2 Wireless-AC VPN.

Популярная линейка маршрутизаторов для малого бизнеса, производимая Cisco Systems, подвержена высокозащищенным уязвимостям. В случае использования уязвимость может позволить удаленному, хотя и прошедшему проверку подлинности, злоумышленнику выполнить код или неожиданно перезапустить затронутые устройства.

Cisco выпустила исправления для недостатка в своих маршрутизаторах RV132W ADSL2 + Wireless-N VPN и маршрутизаторах RV134W VDSL2 Wireless-AC VPN. Эти маршрутизаторы описываются Cisco как готовые к работе модели, предназначенные для небольших или домашних офисов, а также для небольших развертываний.

Уязвимость (CVE-2021-1287) возникает из-за проблемы в веб-интерфейсе управления маршрутизаторами. По шкале CVSS он занимает 7,2 балла из 10, что делает его серьезным.

«Успешный эксплойт может позволить злоумышленнику выполнить произвольный код от имени пользователя root в базовой операционной системе или вызвать перезагрузку устройства, что приведет к отказу в обслуживании (DoS) на пораженном устройстве», - заявила Cisco в среду.

Уязвимость маршрутизатора Cisco

Уязвимость связана с тем, что веб-интерфейс управления маршрутизаторами неправильно проверяет вводимые пользователем данные. Злоумышленник может воспользоваться этой уязвимостью, отправив обработанные HTTP-запросы на уязвимое устройство, однако следует отметить, что злоумышленнику необходимо сначала пройти аутентификацию на устройстве (что может быть достигнуто, например, с помощью фишинг-атаки или другой злонамеренной атаки).

Затрагиваются маршрутизаторы RV132W ADSL2 + Wireless-N VPN, на которых установлена прошивка более ранней, чем версия 1.0.1.15 (которая исправлена); и на маршрутизаторах RV134W VDSL2 Wireless-AC VPN с микропрограммой более ранней версии, чем версия 1.0.1.21 (фиксированная версия). Шичжи Хэ из Уханьского университета сообщил о недостатке.

«Группе реагирования на инциденты, связанные с безопасностью продуктов Cisco (PSIRT), неизвестно о каких-либо публичных объявлениях или злонамеренном использовании уязвимости, описанной в этом информационном сообщении», - заявила Cisco.

Недостатки Cisco: исправления, выпущенные в этом году

Патч является последним от Cisco в этом году. В феврале Cisco выпустила исправления критических дыр в своей линейке VPN-маршрутизаторов для малого бизнеса, которые могут быть использованы удаленными злоумышленниками, не прошедшими проверку подлинности, для просмотра или изменения данных, а также для выполнения других несанкционированных действий на маршрутизаторах.

В 2021 году Cisco также устранила различные уязвимости в своей линейке продуктов, в том числе многочисленные критические уязвимости в решениях программно-конфигурируемых сетей для глобальных сетей (SD-WAN) для бизнес-пользователей, а также серьезный недостаток в своей интеллектуальной сети Wi-Fi. Решение Fi для розничных продавцов, которое может позволить удаленному злоумышленнику изменить пароль любого пользователя учетной записи в уязвимых системах». ***(Lindsey O'Donnell. Cisco Plugs Security Hole in Small Business Routers // Threatpost (https://threatpost.com/cisco-security-hole-small-business-routers/164859/). 17.03.2021).***

***

«Дыра в безопасности в плагине Plus Addons for Elementor использовалась в активных атаках нулевого дня до выпуска патча.

Плагин Plus Addons for Elementor для WordPress имеет критическую уязвимость безопасности, которую злоумышленники могут использовать, чтобы быстро, легко и удаленно захватить веб-сайт.

Плагин, у которого, по словам разработчика, установлено более 30 000 активных установок, позволяет владельцам сайтов создавать различные виджеты, ориентированные на пользователя, для своих веб-сайтов, включая логины пользователей и формы регистрации, которые можно добавить на страницу Elementor. Elementor - это инструмент для создания сайтов на WordPress.

Ошибка (CVE-2021-24175) представляет собой проблему повышения привилегий и обхода аутентификации, которая существует в этой функции

регистрационной формы Plus Addons для Elementor. Он получил оценку 9,8 по шкале уязвимости CVSS, что делает его критическим по серьезности.

«К сожалению, эта функция была неправильно настроена и позволила злоумышленникам зарегистрироваться как пользователь с правами администратора или войти в систему как существующий пользователь с правами администратора», - сообщают исследователи Wordfence. Они добавили, что это происходит из-за неработающего управления сеансом, но не предоставили дополнительных технических деталей.

Ошибка нулевого дня

Впервые об ошибке WPScan сообщила компания Seravo, занимающаяся веб-хостингом, как о «нулевом дне» под активными атаками киберпреступников.

«Плагин активно используется злоумышленниками для обхода аутентификации, позволяя неаутентифицированным пользователям входить в систему как любой пользователь (включая администратора), просто предоставляя соответствующее имя пользователя, а также создавая учетные записи с произвольными ролями, такими как администратор.

Что касается того, как киберпреступники используют эксплойт, Wordfence отметил, что индикаторы взлома указывают на то, что злоумышленники создают привилегированные учетные записи, а затем используют их для дальнейшего взлома сайта.

К сожалению, уязвимость все еще может быть использована, даже если нет активной страницы входа или регистрации, созданной с помощью плагина, и даже если регистрация и вход в систему приостановлены или отключены.

«Это означает, что любой сайт, на котором запущен этот плагин, уязвим для взлома», - говорится в публикации Wordfence.

Как исправить надстройки Plus для уязвимости Elementor Security

По словам Wordfence, администраторы сайта должны обновить до версии 4.1.7 The Plus Addons for Elementor, чтобы избежать компрометации, и они должны проверить наличие «любых непредвиденных административных пользователей или плагинов, которые вы не устанавливали». Компания добавила, что в Plus Addons для Elementor Lite нет такой уязвимости.

«Если вы используете плагин Plus Addons for Elementor, мы настоятельно рекомендуем вам деактивировать и полностью удалить плагин, пока эта уязвимость не будет исправлена», - заявили исследователи. «Если бесплатной версии будет достаточно, вы можете пока перейти на эту версию».

Проблемы с плагином WordPress сохраняются

Плагины WordPress продолжают предлагать злоумышленникам привлекательные возможности для атак.

В январе исследователи предупредили о двух уязвимостях (одна критическая) в плагине WordPress под названием Orbit Fox, который может позволить злоумышленникам внедрить вредоносный код в уязвимые веб-сайты и / или получить контроль над веб-сайтом.

Также в этом месяце было обнаружено, что плагин под названием PopUp Builder, используемый веб-сайтами WordPress для создания всплывающих окон для подписок на информационные бюллетени, имеет уязвимость, которую

злоумышленники могут использовать для отправки информационных бюллетеней с настраиваемым контентом или для удаления или импорта подписчиков на информационные бюллетени.

А в феврале была обнаружена непропатченная, сохраненная ошибка безопасности межсайтового скриптинга (XSS), которая потенциально могла затронуть 50 000 пользователей плагина Contact Form 7 Style». ***(Tara Seals. Cyberattackers Exploiting Critical WordPress Plugin Bug // Threatpost (https://threatpost.com/cyberattackers-exploiting-critical-wordpress-plugin-bug/164663/). 10.03.2021).***

***

«Критические недостатки существуют в Adobe Framemaker, Connect и настольном приложении Creative Cloud для Windows.

Adobe выпустила исправления для множества критических уязвимостей безопасности, которые в случае эксплуатации могут привести к выполнению произвольного кода в уязвимых системах Windows.

Затронутые продукты включают процессор документов Adobe Framemaker, предназначенный для написания и редактирования больших или сложных документов; Программное обеспечение Adobe Connect, используемое для удаленных веб-конференций; и программный пакет Adobe Creative Cloud для редактирования видео.

«Adobe не известно о каких-либо уязвимостях для решения каких-либо проблем, решаемых в этих обновлениях», - заявил представитель Adobe.

Хотя эти уязвимости классифицируются как недостатки критической степени серьезности, важно отметить, что Adobe присвоила им рейтинг «приоритет 3». Это означает, что обновление «устраняет уязвимости в продукте, который исторически не был целью злоумышленников», и что администраторам настоятельно рекомендуется «устанавливать обновление по своему усмотрению».

Недостаток безопасности Adobe Framemaker

Adobe исправила критическую ошибку (CVE-2021-21056) в Framemaker, которая могла допускать выполнение произвольного кода в случае взлома. Уязвимость представляет собой ошибку чтения за пределами допустимого диапазона; который представляет собой тип ошибки переполнения буфера, когда программное обеспечение считывает данные за пределами предполагаемого буфера. Злоумышленник, который может считывать данные, находящиеся за пределами памяти, может получить «секретные значения» (например, адреса памяти), которые в конечном итоге позволят ему выполнить код или отказ в обслуживании.

Adobe Framemaker версии 2019.0.8 и ниже (для Windows) подвержены уязвимости; патч выпущен в версии 2020.0.2. Фрэнсис Провенчер, работающий с Trend Micro в рамках программы Zero Day Initiative, обнаружил ошибку.

Приложение Creative Cloud для настольных ПК для Windows

Adobe также исправила три критические уязвимости в ПК-версии приложения Adobe Creative Cloud для пользователей Windows.

Два из трех критических недостатков могут сделать возможным выполнение произвольного кода: один из них (CVE-2021-21068) проистекает из произвольной дыры для перезаписи файла, а другой (CVE-2021-21078) существует из-за ошибки внедрения команды ОС. Третий критический недостаток (CVE-2021-21069) связан с неправильной проверкой ввода и может позволить злоумышленнику получить повышенные привилегии.

Затронуто настольное приложение Creative Cloud версии 5.3 и более ранние; исправления выпущены в версии 5.4.

Критические и важные недостатки Adobe Connect

В Adobe Connect было исправлено несколько критических и важных ошибок.

Одна критическая ошибка (CVE-2021-21078) возникла из-за неправильной проверки ввода; это могло позволить выполнение произвольного кода.

Также были исправлены три важных недостатка межсайтового скриптинга (XSS) (CVE-2021-21079, CVE-2021-21080, CVE-2021-21081). Они могут позволить произвольное выполнение JavaScript в браузере жертвы в случае взлома.

Это касается Adobe Connect версии 11.0.5 и более ранних; исправление выпущено в версии 11.2.

Обновления безопасности Adobe Connect

Регулярно планируемые в этом месяце исправления безопасности происходят вслед за активно эксплуатируемой критической уязвимостью в феврале, которую злоумышленники использовали для нацеливания на пользователей Adobe Reader в Windows.

Эта ошибка (CVE-2021-21017) использовалась в «ограниченных атаках», согласно ежемесячному информационному бюллетеню Adobe, содержащему его регулярные февральские обновления. Рассматриваемая уязвимость - это ошибка переполнения буфера на основе кучи критической степени серьезности». ***(Lindsey O'Donnell. Adobe Critical Code-Execution Flaws Plague Windows Users // Threatpost (https://threatpost.com/adobe-critical-flaws-windows/164611/). 09.03.2021).***

***

«Производитель средств безопасности и автоматизации F5 предупредил о семи уязвимостях класса patch-ASAP в своих продуктах для сетевой безопасности и обработки трафика Big-IP, а также еще о 14 уязвимостях, которые стоит исправить…

Большинство ошибок касается TMUI - пользовательского интерфейса управления трафиком, с которым пользователи работают для управления продуктами F5, - и их можно использовать для удаленного выполнения кода, атак типа «отказ в обслуживании» или полного захвата устройства; иногда все три. API-интерфейс iControl REST, который F5 предлагает для автоматизации своих продуктов, также проблематичен.

Для начала, есть CVE-2021-22987, который имеет 9,9 балла по десятибалльной шкале серьезности CVSS, поскольку он «позволяет аутентифицированным пользователям с сетевым доступом к утилите настройки через порт управления BIG-IP или собственные IP-адреса., для выполнения произвольных системных команд, создания или удаления файлов или отключения

служб». Администраторам сообщают, что этот недостаток позволяет «полностью взломать систему и выйти из режима устройства». Обратите внимание, что это можно использовать только через плоскость управления, и для этого требуется, чтобы злоумышленник имел действительный логин - возможно, злоумышленник или кто-то, использующий украденные учетные данные.

CVE-2021-22986 с рейтингом всего 9,8 «позволяет неаутентифицированным злоумышленникам, имеющим сетевой доступ к интерфейсу iControl REST, через интерфейс управления BIG-IP и собственные IP-адреса, выполнять произвольные системные команды, создавать или удалять файлы, а также отключать Сервисы." Возможным последствием снова является полная компрометация системы. Мы отмечаем, что для этого не требуется аутентификация, также можно использовать только через плоскость управления, и все же оценка ниже, чем '22987. Причина в том, что последняя ошибка, по-видимому, изменяет область безопасности при эксплуатации.

CVE-2021-22991 и CVE-2021-22992 набрали всего 9,0 балла каждый.

Если ваша установка уязвима для «22991», «нераскрытые запросы к виртуальному серверу могут неправильно обрабатываться нормализацией URI микроядра управления трафиком (TMM), что может вызвать переполнение буфера, что приведет к DoS-атаке». Нарушение управления доступом на основе URL или другие возможные последствия - разрешение удаленного выполнения кода (RCE). Феликс Вильгельм из Google Project Zero предоставляет более подробную техническую информацию здесь.

Ошибка «22992» - тоже потенциальный ужастик. F5 сообщает: «Вредоносный HTTP-ответ на виртуальный сервер Advanced WAF / ASM со страницей входа, настроенной в его политике, может вызвать переполнение буфера, что приведет к DoS-атаке. В определенных ситуациях он может разрешить удаленное выполнение кода (RCE), что приведет к полной компрометации системы». У Вильгельма из Google есть экспериментальный эксплойт и дополнительная информация здесь.

Вы еще не вышли из леса, дорогой читатель, потому что следующий в списке имеет рейтинг CVSS 8,8, так что это все еще очень неприятно. CVE-2021-22988 означает, что пользовательский интерфейс управления трафиком BIG-IP «имеет уязвимость для аутентифицированного удаленного выполнения команд на нераскрытых страницах».

CVE-2021-22989 сдерживает ужас своим рейтингом 8,0, но позволяет «высокопривилегированным пользователям, прошедшим проверку подлинности… выполнять произвольные системные команды, создавать или удалять файлы или отключать службы». Снова возможна полная компрометация системы и выход из режима устройства.

Коротышка помета с рейтингом 6,6 - CVE-2021-22990.

Исправления будут внесены, если вы обновите BIG-IP до версий 16.0.1.1, 15.1.2.1, 14.1.4, 13.1.3.6, 12.1.5.3 и 11.6.5.3. CVE-2021-22986 влияет на другой продукт F5, BIG-IQ, и может быть исправлен путем обновления до версий 8.0.0, 7.1.0.3 и 7.0.0.2.

Предупреждение F5 о семи гадостях также упоминается в сообщении о том, что компания выпустила подробную информацию о 14 других CVE, не связанных с описанными выше. Они перечислены здесь.

Семь основных ошибок настолько серьезны, что Американское агентство по киберпространству и инфраструктуре (CISA) выпустило рекомендацию, в которой «призывает пользователей и администраторов ознакомиться с рекомендациями F5 и как можно скорее установить обновленное программное обеспечение». Возможно, это связано с тем, что в прошлом иностранные злоумышленники использовали дыры F5, чтобы проникнуть в сети, принадлежащие дяде Сэму и крупному бизнесу.

CISA и ФБР также опубликовали совместный информационный бюллетень по кибербезопасности [PDF] с подробным описанием разрушительных ошибок на прошлой неделе в Microsoft Exchange Server.

В досье говорится, что наблюдаемые атаки, использующие недостатки Exchange, «согласуются с предыдущими целевыми действиями китайских киберпреступников».

«Незаконно полученная бизнес-информация, передовые технологии и данные исследований могут подорвать бизнес-операции и развитие исследований многих американских компаний и учреждений», - говорится в документе.

В нем указывается, что «местные органы власти, академические учреждения, неправительственные организации и коммерческие предприятия в различных отраслях промышленности, включая сельское хозяйство, биотехнологии, аэрокосмическую промышленность, оборону, юридические услуги, электроэнергетику и фармацевтику» подверглись атакам из-за ошибок Microsoft». ***(Simon Sharwood. Now it is F5's turn to reveal critical security bugs – and the Feds were quick to sound the alarm on these BIG-IP flaws // The Register (https://www.theregister.com/2021/03/11/f5_critical_flaws/). 11.03.2021).***

***

«Google Chrome заблокирует доступ браузера к TCP-порту 554 для защиты от атак с использованием уязвимости NAT Slipstreaming 2.0.

В прошлом году исследователи безопасности раскрыли новую версию уязвимости NAT Slipstreaming, которая позволяет вредоносным скриптам обходить брандмауэр NAT посетителя веб-сайта и получать доступ к любому порту TCP / UDP во внутренней сети посетителя.

Поскольку эта уязвимость работает только на определенных портах, контролируемых шлюзом уровня приложений (ALG) маршрутизатора, разработчики браузеров, включая Google, Safari и Mozilla, блокируют уязвимые порты, на которые не поступает большой трафик.

Когда уязвимость была впервые обнаружена, Google Chrome 87 начал блокировать доступ HTTP и HTTPS к TCP-портам 5060 и 5061 для защиты от уязвимости.

В январе 2021 года Google заблокировал доступ по протоколам HTTP, HTTPS и FTP к дополнительным семи портам: портам 69, 137, 161, 1719, 1720, 1723 и 6566.

В прошлом Google также блокировал порт 554, но снял блокировку после жалоб от корпоративных пользователей.

«Раньше Chrome ненадолго блокировал порт 554, но он был разблокирован из-за жалоб корпоративных пользователей. Однако теперь мы достигли приблизительного согласия на https://github.com/whatwg/fetch/pull/1148, чтобы заблокировать 554», - инженер Chromium. Об этом заявил сегодня Адам Райс.

Разработчики Google и Safari также обсуждают блокировку доступа к порту 10080, который Firefox уже блокирует, но не решаются из-за законных запросов веб-браузера к этому порту…

Firefox 84+ и Safari уже блокируют порт 554 в своих браузерах». ***(Lawrence Abrams. Google Chrome to block port 554 to stop NAT Slipstreaming attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/google-chrome-to-block-port-554-to-stop-nat-slipstreaming-attacks/). 08.03.2021).***

***

«Злоумышленники нацелены на приложения Amazon, Zillow, Lyft и Slack NodeJS, используя новую уязвимость Dependency Confusion, чтобы украсть файлы паролей Linux / Unix и открыть обратные оболочки обратно для злоумышленников.

…исследователь безопасности Алекс Бирсан получил вознаграждение за обнаружение ошибок от 35 компаний, использовав новую уязвимость в инструментах разработки с открытым исходным кодом.

Эта уязвимость работает, когда злоумышленники создают пакеты, использующие те же имена, что и внутренние репозитории или компоненты компании. При размещении в общедоступных репозиториях, включая npm, PyPI и RubyGems, менеджеры зависимостей будут использовать пакеты в общедоступном репозитории, а не внутренние пакеты компании при создании приложения.

Эта «путаница с зависимостями» позволит злоумышленнику внедрить свой собственный вредоносный код во внутреннее приложение при атаке цепочки поставок.

Злоумышленники начинают использовать путаницу в зависимостях

После нашего отчета BleepingComputer ждал, пока злоумышленники воспользуются этой новой уязвимостью для доставки вредоносных пакетов.

Хотя мы видели, как многочисленные исследователи безопасности выдавали себя за работу Бирсана, создавая безобидные PoC, чтобы заработать вознаграждение за ошибки, мы не видели никаких злонамеренных действий.

Так было до сегодняшнего дня, когда компания Sonatype по обеспечению безопасности с открытым исходным кодом обнаружила вредоносные пакеты, нацеленные на приложения, связанные с Amazon, Zillow, Lyft и Slack, для кражи паролей и открытия удаленных командных оболочек.

«Я начал задаваться вопросом, когда мы увидим злоумышленника, который воспользуется текущей ситуацией. Наконец, мы заметили одного».

«Я не могу представить себе сценарий, в котором я собираюсь отправить PoC для программы вознаграждения за ошибки, которая на самом деле вредит

организации. Взятие их файла / etc / shadow определенно вредно», - сказал исследователь безопасности Sonatype Хуан Агирре в новом отчете.

Эти вредоносные пакеты называются «AMZN», «ZG-аренда», «Lyft-набор данных-SDK», «бессерверной-отвисшей приложение» и использовать подобные имена, как известных репозиториев на GitHub [1, 2] и других проектов.

Когда злоумышленники создавали свои вредоносные NPM, они использовали оригинальные PoC Бирсана в качестве шаблона, но добавляли вредоносный код.

«Они начинают практически с той же кодовой базы, что и PoC, выпущенный исследователем Алексом Бирсаном, и постепенно начинают проявлять творческий подход», - объясняет Агирре.

Например, пакеты NPM 'amzn' и 'zg-rentals' не только украдут файл паролей / etc / shadows (строка 5 ниже) и отправят его обратно злоумышленникам (строка 42), но также откроют удаленную оболочку (строка 26), предоставляя злоумышленникам полный доступ к системе.

Lyft-dataset-sdk и serverless-slack-app, похоже, принадлежат другому автору, и вместо этого крадут файл .bash_history профилей Linux и отправляют его на удаленный хост под контролем злоумышленника.

Вы можете спросить, зачем злоумышленнику украсть файл .bash_history?

Поскольку файл истории содержит список всех команд, введенных вами в оболочке, включая пароли, переданные в качестве аргументов, кража файла .bash_history - это известный метод, используемый злоумышленниками для сбора учетных данных.

Учитывая открытую и общедоступную природу репозиториев и простоту создания атак путаницы зависимостей, мы должны ожидать продолжения атак этого типа до тех пор, пока разработчики приложений не защитят свои файлы конфигурации.

Корпорация Майкрософт создала технический документ под названием «3 способа снижения риска при использовании каналов частных пакетов», в котором содержатся советы по предотвращению подобных атак на цепочку поставок.

Sonatype также создал сценарий, который пользователи Nexus Repository Manager могут использовать, чтобы проверить, названы ли их частные зависимости в честь существующих пакетов в общедоступных репозиториях». ***(Lawrence Abrams. Malicious NPM packages target Amazon, Slack with new dependency attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/malicious-npm-packages-target-amazon-slack-with-new-dependency-attacks/). 02.03.2021).***

***

«Исследователи безопасности Майкл Страметц (Michael Strametz) и Маттиас Диг (Matthias Deeg) из компании SySS обнаружили уязвимость (CVE-2021-28133) функции совместного использования экрана Zoom, из-за которой конфиденциальная информация пользователей может быть передана другим участникам звонка.

Обнаруженная проблема позволяет выявлять содержимое приложений, которые не используются совместно, а лишь на короткое время, затрудняя эксплуатацию уязвимости в реальных атаках. Функция совместного использования

экрана в Zoom позволяет пользователям коллективно использовать весь рабочий стол или экран телефона или ограничить совместное использование одним или несколькими конкретными приложениями или частью экрана. Проблема возникает из-за того, что второе приложение, запущенное поверх уже совместно используемого приложения, может раскрыть его содержимое в течение короткого периода времени.

«Когда пользователь Zoom предоставляет доступ к определенному окну приложения с помощью функции «поделиться экраном», другие участники встречи могут на короткое время увидеть содержимое других окон приложений», — отметили исследователи.

Эксперты обнаружили проблему в версиях Zoom 5.4.3 и 5.5.4 для ОС Windows и Linux и сообщили компании о своих находках 2 декабря 2020 года. С тех пор прошло уже три месяца, однако компания не выпустила исправление для данной уязвимости. Предположительно, это может быть связано со сложностью ее эксплуатации в реальных атаках». ***(В функции совместного использования экрана Zoom обнаружена уязвимость // SecurityLab.ru (https://www.securitylab.ru/news/517585.php). 19.03.2021).***

***

«Специалист издания Motherboard обнаружил опасную проблему, эксплуатация которой позволяет злоумышленникам тайно перенаправлять на свой номер SMS-сообщения жертв путем приобретения соответствующих услуг у телекоммуникационных компаний.

В рамках атаки преступники пользуются услугами компаний, которые помогают предприятиям проводить SMS-маркетинг и массовую рассылку сообщений, чтобы незаметно перенаправлять текстовые сообщения и получать доступ к любым кодам двухфакторной авторизации или ссылкам в текстовых сообщениях.

Некоторые компании позволяют перенаправлять SMS-сообщения на другой номер, не запрашивая разрешения для данной операции и даже не уведомляя пользователя о том, что его текстовые сообщения теперь отправляются кому-то другому.

Исследователь Джозеф Кокс (Joseph Cox) попросил своего знакомого ИБ-эксперта атаковать его номер и перенаправить SMS-сообщения на другой номер. Специалист воспользовался сервисом компании Sakari, и подобная атака обошлась ему всего в $16.

«Я использовал предоплаченную карту, чтобы приобрести месячную подписку за $16, а затем получил возможность похитить номер, просто заполнив форму LOA (Letter of Authorization) фальшивой информацией», — пояснил эксперт.

Letter of Authorization представляет собой документ, в котором говорится, что подписывающая сторона имеет право менять телефонные номера.

Хакеры нашли множество способов использования SMS и сотовых систем для доступа к чужим сообщениям — подмена SIM-карты и атаки на сети SS7 широко используются уже несколько лет, а иногда даже используются против высокопоставленных целей. Подмену SIM-карты довольно легко обнаружить,

поскольку телефон отключается от сотовой сети, но с перенаправлением SMS может пройти довольно много времени, прежде чем пользователь заметит атаку, предоставляя злоумышленникам возможность скомпрометировать учетные записи». ***(Хакеры могут перенаправлять на свой номер SMS-сообщения жертв всего за $16 // SecurityLab.ru (https://www.securitylab.ru/news/517484.php). 16.03.2021).***

***

«Microsoft Teams стала основной платформой в новую эру «работы из дома», и, отражая ее растущее значение, Microsoft запустила программу вознаграждений за ошибки для исследователей, которые обнаруживают недостатки безопасности в программном обеспечении для настольных ПК.

Microsoft предлагает до 30 000 долларов исследователям в области безопасности в рамках вознаграждения за обнаружение ошибок в Teams с «наградами на основе сценариев за уязвимости», если они имеют большое влияние на конфиденциальность и безопасность клиентов. Награды начинаются от 6000 долларов.

Главный приз отражает растущее значение Microsoft Teams, у которого 115 миллионов активных пользователей в день.

Награда за ошибку распространяется только на настольный клиент Microsoft Teams, который доступен для Windows 10, macOS и Linux. Бонус не распространяется на приложение Teams для настольных браузеров или собственные мобильные приложения для iOS и Android.

Награда $ 30000 доступна для исследователей, которые могут четко очертить удаленный запуск кода ошибки с использованием нативного кода в контексте текущего пользователя, без взаимодействия с пользователем.

Microsoft также предлагает 15 000 долларов за ошибку, которая позволяет злоумышленнику получить учетные данные для аутентификации для других пользователей, но фишинг исключен.

Он предлагает 10 000 долларов за недостатки межсайтового скриптинга (XSS) или другое удаленное внедрение кода, которое позволяет злоумышленнику выполнять произвольные скрипты в контексте team.microsoft.com или team.live.com без взаимодействия с пользователем. Столько же доступно для исследователей, которые могут продемонстрировать способ повышения привилегий, перескакивая через границы Windows и пользователя.

Вознаграждение в размере 6000 долларов доступно исследователям, обнаружившим XSS или другую «инъекцию кода, дающую возможность выполнять произвольные сценарии в контексте team.microsoft.com или team.live.com с минимальным взаимодействием с пользователем».

Microsoft также предлагает общие награды за настольное приложение Teams, которые выходят за рамки наград, основанных на сценариях, с вознаграждением до 15 000 долларов…». ***(Liam Tung. Microsoft Teams now has its own bug bounties for researchers who can spot security flaws // ZDNet (https://www.zdnet.com/article/microsoft-teams-now-has-its-own-bug-bounties-for-researchers-who-can-spot-security-flaws/). 25.03.2021).***

***

«Два из пяти предприятий подверглись кибератакам в течение прошлого года, причем одна конкретная угроза была наиболее распространенной.

А рост удаленной работы в сочетании с небольшим сокращением числа организаций, использующих инструменты мониторинга безопасности для выявления аномальной активности, может означать, что фактическое количество организаций, ставших жертвами киберпреступности, выше - и они просто не знают, что были скомпрометированы. все же.

Цифры подробно описаны в ежегодном обзоре нарушений кибербезопасности Департамента цифровых технологий, культуры, СМИ и спорта (DCMS), который показывает, как компании подходят к кибербезопасности и последствиям атак.

Отчет за 2021 год был выпущен после года, когда организациям пришлось быстро адаптироваться к удаленной работе, что потенциально повысило кибер-риск, поскольку сотрудники больше не были защищены корпоративными брандмауэрами, а работали из своих домов.

Более 80% организаций, выявивших кибератаки в течение прошлого года, подвергались фишинговым электронным письмам, при этом киберпреступники использовали вредоносные сообщения, пытаясь удалить вредоносные программы или заставить людей переходить по вредоносным ссылкам.

Чуть более четверти организаций выявили атаки на электронную почту, при которых злоумышленники выдавали себя за людей или компании в Интернете - это могла быть либо попытка кражи учетных данных, либо попытки взлома корпоративной электронной почты, когда киберпреступники пытаются обманом заставить сотрудников совершить крупные финансовые переводы, часто притворяясь. быть важной деловой сделкой или контрактом.

Электронная почта долгое время была обычным средством проведения кибератак, но переход к удаленной работе за последний год означает, что люди больше полагаются на нее для совместной работы на рабочем месте. В отчете предполагается, что это может быть причиной того, что некоторые компании не могут выявлять кибератаки или утечки данных.

Чуть более одной из двадцати организаций заявили, что они выявили попытку атаки с использованием программ-вымогателей.

Хотя большинство организаций, выявивших кибератаку, пытались принять меры, включая дополнительное обучение персонала, обновление антивирусного программного обеспечения, изменение конфигурации брандмауэра или установку другого нового программного обеспечения, чуть более трети вообще не предприняла никаких действий после обнаружения инцидент.

В отчете также отмечается рост числа организаций, которые в той или иной форме заключили киберстрахование, чтобы покрыть финансовые расходы, связанные с кибератаками.

В отчете дается несколько рекомендаций организациям по обеспечению безопасности и устойчивости их сетей к кибератакам. К ним относятся защита

учетных записей с помощью многофакторной аутентификации и повышение осведомленности персонала о проблемах кибербезопасности с помощью обучения.

В отчете также рекомендуется, чтобы организации предприняли дополнительные действия в отношении управления рисками цепочки поставок, чтобы обеспечить лучшую защиту от атак, которые могут попытаться использовать цепочку поставок в качестве средства доступа к сети.

«Для организаций, правления и ИТ-специалистов важно осознавать, что хорошая кибербезопасность способствует повышению устойчивости бизнеса. Это не всегда ценилось во время пандемии, когда упор на краткосрочную непрерывность бизнеса и ИТ-услуг иногда затмевает дискуссии о кибербезопасности. ", - говорится в сообщении.

«После выхода из пандемии у команд по кибербезопасности может появиться возможность переосмыслить эти дискуссии, чтобы показать, что кибербезопасность является неотъемлемым компонентом устойчивости бизнеса», - заключил он». ***(Danny Palmer. Four out of five companies say they've spotted this cyberattack. Plenty still fall victim to it // ZDNet (https://www.zdnet.com/article/four-out-of-five-companies-say-theyve-spotted-this-cyber-attack-plenty-still-fall-victim-to-it/). 25.03.2021).***

***

«В плагине Facebook для WordPress были исправлены две серьезные уязвимости.

На этой неделе команда Wordfence Threat Intelligence сообщила, что ошибки влияют на Facebook для WordPress, ранее известный как Official Facebook Pixel.

Плагин, используемый для отслеживания действий пользователей при посещении страницы и отслеживания посещаемости сайта, был установлен на более чем 500 000 веб-сайтов.

22 декабря исследователи кибербезопасности в частном порядке раскрыли поставщику критическую уязвимость, которой была присвоена оценка серьезности CVSS 9. Уязвимость, описанная как внедрение объекта PHP, была обнаружена в функции run_action () программного обеспечения.

Если был сгенерирован действительный одноразовый номер - например, с помощью пользовательского сценария - злоумышленник может предоставить подключаемому модулю объекты PHP для злонамеренных целей и зайти так далеко, что загрузит файлы на уязвимый веб-сайт и добьется удаленного выполнения кода (RCE).

«Этот недостаток позволил неаутентифицированным злоумышленникам, имеющим доступ к секретным солям и ключам сайта, добиться удаленного выполнения кода за счет уязвимости десериализации», - заявляет команда.

Вторая уязвимость, считающаяся очень важной, была обнаружена 27 января. Недостаток защиты от подделки межсайтовых запросов, приводящий к проблеме межсайтового скриптинга, был обнаружен случайно во время ребрендинга плагина.

Когда программное обеспечение было обновлено, была введена функция AJAX, чтобы упростить интеграцию плагинов. Однако проблема проверки разрешений в функции открыла для злоумышленников возможность создавать

запросы, которые могут быть выполнены, «если они смогут обманом заставить администратора выполнить действие при аутентификации на целевом сайте», согласно Wordfence.

«Действие может быть использовано злоумышленником для обновления настроек плагина, чтобы он указывал на его собственную консоль Facebook Pixel и украл данные метрик для сайта», - заявляет команда. «Что еще хуже, поскольку не было никакой дезинфекции сохраненных настроек, злоумышленник мог внедрить вредоносный JavaScript в значения настроек».

Вредоносный JavaScript может, например, использоваться для создания бэкдоров в темах или создания новых учетных записей администратора для взлома целых веб-сайтов.

Отчеты были приняты командой безопасности Facebook, и 6 января было выпущено исправление для первой уязвимости, а 12 февраля - второе исправление. Однако исправление для второй ошибки потребовало настройки, и полное исправление не было опубликовано до 17 февраля.

Обе уязвимости были обновлены в версии 3.0.4, поэтому веб-мастерам рекомендуется обновить доступную версию плагина до последней версии 3.0.5…». ***(Charlie Osborne. Severe vulnerabilities patched in Facebook for WordPress Plugin // ZDNet (https://www.zdnet.com/article/severe-vulnerabilities-patched-in-facebook-for-wordpress-plugin/). 25.03.2021).***

***

«Сетевая маска популярной библиотеки npm имеет критическую сетевую уязвимость.

netmask часто используется сотнями тысяч приложений для анализа адресов IPv4 и блоков CIDR или их сравнения.

Компонент получает более 3 миллионов загрузок еженедельно, и на сегодняшний день он набрал более 238 миллионов загрузок за время его существования. Кроме того, около 278000 репозиториев GitHub зависят от сетевой маски.

Ошибка, присутствующая в библиотеке, означает, что при разборе IP-адреса с начальным нулем сетевая маска видит другой IP-адрес из-за неправильной проверки на месте.

Ведущий ноль изменяет IP-адрес

Сегодня исследователи в области безопасности Виктор Viale, Sick коды, Ник Sahler, Келли Kaoudis и Джон Джексон раскрыли изъян в популярной NETMASK библиотеке.

Уязвимость, отслеживаемая как CVE-2021-28918, а в последнее время как CVE-2021-29418, касается того, как сетевая маска обрабатывает IP-адреса смешанного формата, или, более конкретно, когда десятичный IPv4-адрес содержит начальный ноль.

IP-адрес может быть представлен в различных форматах, включая шестнадцатеричный и целочисленный, хотя наиболее часто встречающиеся адреса IPv4 выражаются в десятичном формате.

Например, IPv4-адрес BleepingComputer, представленный в десятичном формате, - 104.20.59.209, но то же самое может быть выражено в восьмеричном формате как 0150.0024.0073.0321.

Допустим, вам дан IP-адрес в десятичном формате 127.0.0.1, который широко понимается как локальный адрес обратной связи или localhost.

Если бы вы поставили перед ним префикс 0, должно ли приложение все равно анализировать 0127.0.0.1 как 127.0.0.1 или что-то еще?

Попробуйте это в своем веб-браузере. В тестах BleepingComputer при вводе 0127.0.0.1/ в адресной строке Chrome браузер рассматривал его как IP-адрес в восьмеричном формате.

При нажатии клавиши ввода или возврата IP фактически изменяется на его десятичный эквивалент 87.0.0.1, именно так большинство приложений должны обрабатывать такие неоднозначные IP-адреса.

Особо следует отметить тот факт, что 127.0.0.1 - это не общедоступный IP-адрес, а адрес обратной связи, однако его неоднозначное представление меняет его на общедоступный IP-адрес, ведущий к другому хосту.

Но в случае сетевой маски библиотеки npm любые ведущие нули будут просто удалены и отброшены.

Согласно исходной спецификации IETF, части адреса IPv4 могут интерпретироваться как восьмеричные, если перед ними стоит префикс «0».

«Но сетевая маска игнорирует это. Она всегда будет рассматривать части как десятичные, а это означает, что если вы попытаетесь проверить принадлежность IP-адреса к диапазону, это будет неправильным для восьмеричного представления адресов IPv4», - сказали Sahler и Viale BleepingComputer в интервью по электронной почте.

Обход Anti-SSRF и черный список для включения удаленного файла

На первый взгляд эта ошибка может показаться незначительной, но если злоумышленник сможет повлиять на ввод IP-адреса, анализируемый приложением, ошибка может привести к различным уязвимостям из-за обхода подделки запросов на стороне сервера (SSRF). к удаленному включению файлов (RFI).

Исследователи поделились различными примерами с BleepingComputer, демонстрирующими то же самое.

«Кто-то запускает сервер узла для очистки входящего запроса или параметра запроса, который должен быть URI, используемым для дальнейшего соединения, выборки ресурсов и т. Д.».

«Злоумышленник создает IP-адрес с некоторыми или всеми октетами в базе 8 в старом представлении JavaScript с префиксом 0».

«Это может быть полезно для SSRF, например, для принудительного подключения сервера к 127.0.0.1 путем передачи 0177.0.0.01. 177 - это основание 8 для 127 в десятичной системе», - сказал Каудис BleepingComputer.

«Хорошим примером является система, которая выявляет веб-перехватчики и проверяет URL-адреса пользователей с помощью проверки сетевой маски на уязвимость для SSRF», - также добавил Виале.

Принимая во внимание, что эта ошибка также может быть использована для включения удаленного файла (RFI), если злоумышленник создает IP-адрес,

который выглядит частным для сетевой маски, из-за того, как сетевая маска преобразует все части IPv4 (октеты) в десятичный формат, но оценивается как общедоступный другие компоненты, - объяснил Каудис BleepingComputer.

В 2018 году у популярного программного проекта curl была обнаружена идентичная ошибка, когда восьмеричные адреса IPv4 обрабатывались как десятичные:

В тестах BleepingComputer при запуске "curl -v 0177.0.0.1" curl подключается к 177.0.0.1, а не к адресу обратной петли 127.0.0.1.

Тогда этичный хакер Николя Грегуар также пролил свет на то, как можно использовать такую уязвимость для обхода списков контроля доступа (ACL) на основе IP.

«Я часто использую эти преобразования, чтобы обойти черные списки анти-SSRF, - сказал Грегуар.

Различные продукты сетевой инфраструктуры и безопасности, такие как брандмауэры веб-приложений, используют сетевую маску для фильтрации IP-адресов, присутствующих в списках блокировки и списках разрешений.

Это также означает, что подобные недостатки, если их не устранить, могут привести к серьезным ошибкам в контроле безопасности периметра.

Ранее Sick Codes, Джексон и Салер выявили похожий недостаток в пакете private-ip, который, как оказалось, также использует сетевую маску в качестве зависимости даже сегодня.

В конечном итоге, говорит Джексон, эта недавно обнаруженная проблема в сетевой маске делает тысячи проектов уязвимыми для обхода SSRF.

«В сетевую маску еженедельно скачиваются миллионы файлов, что сильно влияет на нее. Это огромная уязвимость в цепочке поставок программного обеспечения».

«Оглядываясь назад, можно сказать, что критичность нашей CVE с частным IP- адресом достигла 9,8, а еженедельно у нас было около 175 000 загрузок», - сказал Джексон BleepingComputer.

Основное беспокойство исследователя вызывает то, что многие проекты, использующие сетевую маску для синтаксического анализа IP-адресов, могут ошибочно полагать, что они защищены от SSRF.

Фиксированная версия выпущена на npm

После ответственного сообщения исследователей об уязвимости разработчик сетевой маски и технический директор Netflix Оливье Пуатри опубликовал серию исправлений [1, 2, 3] для ошибки на GitHub, а также тестовые примеры, подтверждающие, что октеты IPv4 с 0 -префиксы обрабатываются как восьмеричные, а не десятичные числа.

Исправление для CVE-2021-28918 было выпущено в версии 2.0.0 сетевой маски при загрузках npm, однако исследователь RyotaK вскоре обнаружил, что исправления неполные.

Таким образом, на этой неделе этой уязвимости был присвоен новый идентификатор CVE-2021-29418, а исправление было добавлено в сетевую маску версии 2.0.1.

Когда его попросили прокомментировать критический характер этой уязвимости, разработчик сказал BleepingComputer, что это зависит от того, как вы определяете «критическую».

«Зависит от того, как вы определяете критическое и как вы используете эту библиотеку. Это не ошибка переполнения буфера или удаленного выполнения».

«Я не могу атаковать ваше приложение, но ослаблю ваш ACL, если он основан на IP-доступе с использованием этой библиотеки».

«Мне еще предстоит представить сценарий, в котором это можно было бы использовать, поскольку в большинстве случаев ACL основаны на IP-адресах, полученных из стека IP, и они никогда не будут использовать уязвимый формат», - сказал Пойтри BleepingComputer.

Пользователям библиотеки netmask npm рекомендуется выполнить обновление до фиксированной версии 2.0.1.

Исследователи раскрыли свои выводы в GitHub консультативной и блоге.

Компонент Perl Net: Netmask также страдал от этого недостатка, и его сопровождающий Жоэль Маслак сегодня выпустил исправление в версии 2.0000.

Разработчикам, использующим версию Perl, рекомендуется убедиться, что их приложения очищают и нормализуют IP-адреса, прежде чем передавать их в качестве входных данных в Netmask, и желательно обновить их до фиксированной версии». ***(Ax Sharma. Critical netmask networking bug impacts thousands of applications // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/critical-netmask-networking-bug-impacts-thousands-of-applications/). 28.03.2021).***

***

«Сегодня проект OpenSSL выпустил рекомендации по двум уязвимостям высокой степени серьезности CVE-2021-3449 и CVE-2021-3450, скрывающимся в продуктах OpenSSL.

OpenSSL - это широко используемая программная библиотека для создания сетевых приложений и серверов, которым необходимо установить безопасную связь.

К этим недостаткам относятся:

CVE-2021-3449: ошибка отказа в обслуживании (DoS) из-за разыменования нулевого указателя, которая влияет только на экземпляры сервера OpenSSL, но не на клиентов.

CVE-2021-3450: ненадлежащая уязвимость при проверке сертификатов центра сертификации (ЦС), которая влияет как на сервер, так и на клиентские экземпляры.

Уязвимость DoS исправлена однострочно

Уязвимость DoS (CVE-2021-3449) на сервере OpenSSL TLS может вызвать сбой сервера, если в ходе повторного согласования клиент отправляет вредоносное сообщение ClientHello.

«Если ClientHello с повторным согласованием TLSv1.2 опускает расширение signature_algorithms (там, где оно присутствовало в исходном ClientHello), но включает расширение signature_algorithms_cert, то разыменование указателя NULL

приведет к сбою и атаке отказа в обслуживании», - говорится в заявлении. консультативный.

Уязвимость затрагивает только серверы OpenSSL с версиями от 1.1.1 до 1.1.1j (оба включительно), на которых включены TLSv1.2 и повторное согласование.

Однако, поскольку это конфигурация по умолчанию для этих версий сервера OpenSSL, многие из активных серверов могут быть потенциально уязвимы. Клиенты OpenSSL не затронуты.

К счастью, все, что потребовалось для исправления этой ошибки DoS, - это однострочное исправление, которое включало установку peer_sigalgslen в ноль.

Уязвимость была обнаружена инженерами Питером Кестле и Самуэлем Сапальски из Nokia, которые также предложили исправление, показанное выше.

Сертификаты, отличные от CA, не могут выдавать сертификаты!

Уязвимость CVE-2021-3450, связанная с обходом проверки сертификатов центра сертификации (CA), связана с флагом X509_V_FLAG_X509_STRICT.

Этот флаг используется OpenSSL, чтобы запретить использование обходных путей для сломанных сертификатов, и строго требует, чтобы сертификаты были проверены на соответствие правилам X509.

Однако из-за ошибки регрессии этой уязвимости подвержены OpenSSL версии 1.1.1h и выше (за исключением фиксированного выпуска 1.1.1k), поскольку в этих версиях этот флаг не установлен по умолчанию.

«Начиная с OpenSSL версии 1.1.1h, в качестве дополнительной строгой проверки была добавлена проверка, запрещающая сертификаты в цепочке, которые имеют явно закодированные параметры эллиптической кривой».

«Ошибка при реализации этой проверки означала, что результат предыдущей проверки, подтверждающей, что сертификаты в цепочке являются действительными сертификатами CA, был перезаписан», - говорится в сообщении.

По сути, это означает, что экземпляры OpenSSL не могут проверить, не должны ли сертификаты, не относящиеся к CA, быть эмитентами других сертификатов, что открывает возможности для использования злоумышленниками этой ошибки.

18 марта 2021 года Бенджамин Кадук из Akamai сообщил об этой уязвимости проекту OpenSSL.

Уязвимость была обнаружена Сян Дингом и другими сотрудниками Akamai, а исправление было разработано Томашем Мразом.

Ни одна из уязвимостей не влияет на OpenSSL 1.0.2.

Обе уязвимости исправлены в OpenSSL 1.1.1k, и пользователям рекомендуется обновиться до этой версии, чтобы защитить свои экземпляры.

Как сообщает BleepingComputer, DHS-CISA призвала системных администраторов в декабре 2020 года исправить еще одну уязвимость OpenSSL DoS.

Поэтому пользователи должны защищать себя от подобных недостатков безопасности, своевременно устанавливая обновления». ***(Ax Sharma. OpenSSL fixes severe DoS, certificate validation vulnerabilities // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/openssl-fixes-severe-dos-certificate-validation-vulnerabilities/). 25.03.2021).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Argon, израильская компания, которая предоставляет решения для обеспечения безопасности процесса разработки программного обеспечения, во вторник объявила о выходе из скрытого режима.

Компания разработала решение, которое обеспечивает возможность видимости, безопасности и целостности, чтобы помочь командам DevOps и безопасности гарантировать, что их среда разработки не будет скомпрометирована.

Argon заявляет, что его продукт позволяет организациям защитить свой конвейер непрерывной интеграции / непрерывной доставки (CI / CD) путем сопоставления инструментов, активов и действий пользователей, чтобы обеспечить видимость всего процесса DevOps и гарантировать, что код не был изменен. Решение может быть интегрировано во многие популярные инструменты разработки программного обеспечения.

Платформа непрерывно отслеживает среду клиента, чтобы выявлять риски безопасности, аномалии и неправильные конфигурации. Выявленные проблемы расставлены по приоритетам, а их устранение автоматизировано согласно с правилами соответствия и передовой практикой.

Стартап привлек более 4 миллионов долларов начального финансирования от Hyperwise Ventures и нескольких неформальных инвесторов в области кибербезопасности…». ***(Eduard Kovacs. Software Development Security Firm Argon Emerges From Stealth Mode // Wired Business Media (https://www.securityweek.com/software-development-security-firm-argon-emerges-stealth-mode?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Securityweek+%28SecurityWeek+RSS+Feed%29). 16.03.2021).***

***

«Twitter в понедельник объявил, что пользователи с включенной двухфакторной аутентификацией (2FA) теперь могут использовать несколько ключей безопасности для защиты своих учетных записей.

Социальная платформа уже некоторое время поддерживает ключи безопасности для пользователей компьютеров, а в декабре 2020 года сделала эту функцию доступной для пользователей iOS и Android…

Чтобы использовать ключи безопасности для защиты учетной записи, пользователям необходимо включить 2FA с помощью текстового сообщения или приложения проверки подлинности, выбрать ключ безопасности, а затем ввести свои пароли при появлении запроса, чтобы начать процесс настройки.

После нажатия кнопки «Пуск» пользователи могут подключить свой физический ключ безопасности либо через порт USB, либо через Bluetooth, после

чего им нужно будет нажать кнопку на ключе, а затем выполнить действия на экране, чтобы завершить процесс установки.

Добавленные ключи безопасности отображаются в разделе «Управление ключами безопасности» в разделе «Двухфакторная аутентификация», что позволяет пользователям легко управлять ими (при необходимости переименовывать, удалять или добавлять новые).

Социальная платформа также указывает, что для добавления или входа в учетную запись Twitter с помощью ключа безопасности необходима последняя версия поддерживаемого браузера (включая Chrome, Edge, Firefox, Opera и Safari)…». ***(Ionut Arghire. Twitter Users Can Now Secure Accounts With Multiple Security Keys // Wired Business Media (https://www.securityweek.com/twitter-users-can-now-secure-accounts-multiple-security-keys?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Securityweek+%28SecurityWeek+RSS+Feed%29). 16.03.2021).***

***

«Полиция объявила тендер на замену своего инструмента CyberAlarm после того, как The Register и исследователи информационной безопасности сообщили о недостатках безопасности в программном обеспечении для ведения журналов.

Объявление о публичном тендере показало, что Национальный совет начальников полиции (NPCC) ищет нового поставщика для «следующей итерации» сети инструментов регистрации угроз, в очевидной замене существующего программного обеспечения.

Победитель нового контракта должен будет создать новый пакет, отвечающий целям распределенной регистрации угроз NPCC - и в слайде, прилагаемом к уведомлению, поясняется, что это включает «перенос текущих системных данных, участников и возможностей в новую службу».

В прошлом году The Register показал, что Pervade и NPCC знали о недостатках безопасности в инструменте, но молча исправляли их, делая вид, что игнорируют исследователя Пола Мура, который выразил свои опасения непосредственно перед проектом, прежде чем обнародовать его.

Некоторые из этих недостатков были менее серьезными, чем другие, но агрессивный и бесполезный ответ CyberAlarm Муру, а также попытки замалчивать его выводы, когда The Register спрашивал о них, выходили далеко за рамки отраслевых норм.

CyberAlarm - это инструмент для сканирования уязвимостей полиции. Его заявленное намерение состоит в том, чтобы предоставить кибер-копам мгновенный обзор текущих сетевых атак, с которыми сталкиваются британские МСП, со второстепенной функцией, чтобы сообщить предприятиям, которые развертывают инструмент, что они подвергаются атаке. Хост-организации развертывают его в демилитаризованной зоне в своих собственных сетях, чтобы полиция могла просматривать типы и объемы подключений.

Главный суперинтендант детективов Эндрю Гулд, ведущий специалист по киберпреступности NPCC и «владелец» CyberAlarm, заявил: «В связи с растущим

спросом на Police CyberAlarm со стороны предприятий по всей стране, дальнейшее финансирование проекта было обеспечено из Home Офис в течение еще 12 месяцев (2020/21) после последнего годового обзора расходов правительства. В соответствии с положениями о закупках мы должны провести новый конкурсный тендер, чтобы определить поставщика для нового 12-месячного контракта».

Гулд был тем человеком, который отправил письма о прекращении и воздержании аналитику информационной безопасности Муру, приказывая ему прекратить анализ CyberAlarm, потому что его выводы «могли нанести значительный и непоправимый ущерб бренду Police CyberAlarm».

Пресс-секретарь CyberAlarm ранее отрицала, что персонал проекта сообщал представителям общественности, что The Register проверил инструмент и предоставил ему чистую справку о состоянии здоровья.

Странность логотипа

CyberAlarm от NPCC также не единственный британский продукт для информационной безопасности под этим названием. Эль Рег поговорил с Домиником Асланом, директором Cyber Alarm Ltd. Эта компания была зарегистрирована до того, как был запущен полицейский инструмент.

Аслан утверждал, что проект CyberAlarm NPCC при запуске сорвал логотип Cyber Alarm. Подтверждая это, он показал ссылку на Wayback Machine. Первый снимок веб-сайта cyberalarm.police.uk показывает характерный логотип с полукругом в центре.

«Очевидно, что логотип - это то, что я заказал сам, а не значок, который я нашел где-то в Интернете», - сказал Аслан, утверждая, что заказал его в марте прошлого года. «Это то, за что я заплатил, и поэтому авторские права принадлежат моему IP».

По словам Аслана, может быть совпадением, что Cyber Alarm Ltd торговала с домена cyberalarm.org, что было довольно странно, когда он заметил, что NPCC зарегистрировала домен cyberalarm.org.uk для себя.

Что касается более широких вопросов интеллектуальной собственности, директор Cyber Alarm Ltd сказал, что ему посоветовали не пытаться регистрировать CyberAlarm в качестве товарного знака, поскольку органы интеллектуальной собственности, вероятно, сочтут его слишком общим.

«Если общественность должна доверять следующей версии CyberAlarm, NPCC должна извлечь уроки из этого фиаско и работать над восстановлением своей потрепанной репутации». ***(Gareth Corfield. Brit cybercops issue tender to rip and replace their formerly flaw-ridden CyberAlarm tool // The Register (https://www.theregister.com/2021/03/10/police_cyberalarm_pervade_software_new_tender/). 10.03.2021).***

***

«Компания Ericom Software, разработчик облачных решений кибербезопасности для безопасного доступа к веб-сайтам и приложениям, анонсировала новую возможность для облачной службы RBI. Интеллектуальная система RBI упрощает развертывание и использование решения

Ericom Zero Trust для просмотра веб-страниц, обеспечивая защиту от таких угроз, как вымогательство, фишинг, кража учетных записей и пр.

Интеллектуальная изоляция Ericom использует данные сети Ericom Threat Intelligence Network для динамической оценки риска запрашиваемых веб-сайтов. Эта сеть нормализует данные об угрозах URL-адресов, поступающие из различных отраслевых источников, и объединяет их с информацией, являющейся собственностью глобального сообщества пользователей Ericom, для получения в реальном времени оценки степени риска каждый раз, когда пользователь пытается зайти на веб-сайт. Сайты с повышенным уровнем риска отправляются в Ericom RBI для безопасной визуализации, предотвращая вредоносные программы на этом сайте от компрометации устройства пользователя.

Ericom RBI обеспечивает загрузку содержимого сайта в удаленном, изолированном облачном контейнере. Когда пользователь переходит на рискованный сайт или нажимает на URL-адрес, встроенный в фишинговый электронный адрес, он абсолютно безопасен, поскольку веб-содержимое не выполняется непосредственно на его устройстве. Никакие вредоносные программы с рискованных сайтов, даже сложные zero-days, не могут заразить устройство, потому что Ericom RBI посылает только безопасную информацию из «облачного» контейнера в браузер устройства.

Сайты, запущенные с URL-адресов электронной почты, могут быть визуализированы в режиме «только для чтения», чтобы предотвратить вход пользователей в учетные данные, обеспечивая дополнительную защиту от фишинга. Кроме того, файлы с изолированных сайтов могут быть дезинфицированы перед передачей на устройства, гарантируя, что вредоносное ПО, находящееся в загружаемых файлах, не сможет скомпрометировать конечные точки. С Ericom пользователи защищены без потери продуктивности, благодаря полностью интерактивному просмотру веб-страниц.

В дополнение к Intelligent Remote Browser Isolation, Ericom анонсировал новую функцию интеграции SIEM для своей службы RBI. Организации, которым требуется долгосрочное хранение журналов по соображениям соответствия, или которые анализируют тенденции своей активности при просмотре веб-сайтов, теперь могут отправлять журналы трафика веб-сайтов и действий по обеспечению соблюдения политик веб-безопасности сторонним SIEM-продуктам.

Ericom также сообщил о продолжающемся расширении своей платформы Ericom Global Cloud, что значительно увеличивает глобальную плотность точек присутствия (PoP) для удовлетворения растущего спроса на услуги безопасности Ericom Zero Trust». ***(Облачный сервис Ericom RBI защищает пользователей от вредоносного контента веб-сайтов // Компьютерное Обозрение(https://ko.com.ua/oblachnyj_servis_ericom_rbi_zashhishhaet_polzovatelej_ot_vredonosnogo_kontenta_veb-sajtov_136664). 16.03.2021).***

***

«Эксперты Positive Technologies проанализировали результаты мониторинга сетевой активности в четырех десятках компаний, где проводились пилотные проекты по внедрению PT Network Attack Discovery

(PT NAD) и комплекса для раннего выявления сложных угроз (PT Anti-APT). (В выборке представлены только те проекты, заказчики которых дали согласие на исследование результатов мониторинга сетевой активности и их публикацию в обезличенном виде). В ходе анализа в большинстве компаний была выявлена подозрительная сетевая активность, а вредоносное ПО было обнаружено в каждой государственной и промышленной организации.

По результатам пилотных проектов в 90% компаний была выявлена подозрительная сетевая активность, например, сокрытие трафика, запуск инструментов сканирования сети, попытки удаленного запуска процессов. Эксперты отмечают, что использование NTA-систем (network traffic analysis – системы анализа сетевого трафика, которые призваны выявлять атаки внутри инфраструктуры и на периметре организации) позволяет не только вовремя обнаружить подозрительные подключения, но и обратиться к истории сетевой активности узла и проверить, не было ли других подобных попыток.

Переход компаний на удаленную работу повлиял и на сетевую активность: выросла доля подключений во внешнюю сеть по протоколу RDP. Такие подключения необходимо тщательно контролировать, поскольку количество атак через протоколы удаленного доступа в 2020 г. выросло втрое.

В ходе пилотных проектов по мониторингу сетевой активности и выявлению сложных угроз в 2020 г. эксперты столкнулись с активностью 36 семейств вредоносного ПО. В частности шифровальщик WannaCry, банковские трояны RTM, Ursnif и Dridex. В 68% анализируемых компаний была выявлена активность вредоносного ПО, при этом ВПО было обнаружено во всех исследуемых государственных и промышленных организациях. В каждой третьей компании были отмечены попытки эксплуатации уязвимостей в ПО». ***(Вредоносное ПО и нарушения регламентов кибербезопасности обнаружены в каждой компании // Компьютерное Обозрение (https://ko.com.ua/vredonosnoe_po_i_narusheniya_reglamentov_kiberbezopasnosti_obnaruzheny_v_kazhdoj_kompanii_136642). 15.03.2021).***

***

«DMARC (Domain-based Message Authentication, Reporting & Conformance) позволяет организациям защищаться от чрезвычайно популярных среди киберпреступников мошеннических писем со спуфингом (подменой) личности отправителя.

Согласно информации из отчёта о тенденциях внедрения DMARC, которые уже пятый год отслеживает фирма Valimail, ежедневно во всем мире отправляется более трёх миллиардов спуфинговых сообщений (1% всего почтового трафика). Это подвергает людей и организации риску кибератак, включая кражу учётных данных, внедрение вредоносного ПО и программ-вымогателей.

Одним из факторов, способствующих распространению этого вектора атак, стал рост удалённой работы. Он приводит к активизации коропоративных коммуникаций по электронной почте, при этом из дома конечным пользователям сложнее проверить, является ли приходящее электронное письмо подлинным.

DMARC — это антиспамовый протокол аутентификации электронной почты, который разрешает отсылку почты только для тех отправителей, кто авторизован в данном домене. Он также включает функцию отчётности для постоянного улучшения защиты.

Анализ, проведённый Valimail, показал, что 1,9% писем от доменов, к которым не применён протокол DMARC, классифицируются как подозрительные, однако внедрение DMARC снижает долю сомнительного почтового трафика почти в пять раз — до 0,4%.

Сегодня, свыше 1,28 млн доменов по всему миру сконфигурированы для DMARC, но только 14% из них защищены от спуфинга политикой принудительного применения этого протокола. Однако среди доменов крупных организаций, в обязательном порядке защищено с помощью DMARC 43,4% (на 3,5% больше, чем год назад)». ***(Рост почтового спуфинга ведёт к ускорению внедрения протокола DMARC // Компьютерное Обозрение (https://ko.com.ua/rost_pochtovogo_spufinga_vedyot_k_uskoreniyu_vnedreniya_protokola_dmarc_136793). 25.03.2021).***

***

«Идея платформы безопасности не нова. Также нет проблем, связанных с безопасностью и разрастанием поставщиков внутри организации. Первоначальная идея межсетевого экрана следующего поколения заключалась в объединении нескольких продуктов в единую платформу для снижения накладных расходов на ИТ и упрощения коммутационных шкафов, которые были переполнены устройствами безопасности. И это сработало. Решения NGFW быстро стали краеугольным камнем для внедрения безопасности практически в каждой организации в мире.

Однако проблемы все еще оставались. Совместимость была одной из них. Для многих из этих решений различные технологии - обычно это сочетание брандмауэра, IPS, VPN, веб-фильтрации, антивирусной защиты и песочницы - на самом деле не работали вместе как единое целостное решение. Многие компоненты используют разные операционные системы и даже имеют отдельные консоли управления. Другой проблемой было качество решений, встроенных в платформу. Поставщик средств безопасности, создавший платформу NGFW, возможно, имел первоклассный межсетевой экран для использования в качестве якорного решения, но затем внес в реестр безопасности второстепенное решение IPS или веб-фильтрации. Бушевали дебаты о ценности платформы NGFW и лучшего в своем классе подхода к обеспечению безопасности.

Сегодня цифровые инновации вызвали полный переворот в традиционной сети. Мультиоблачные среды, центры обработки данных, состоящие как из физической, так и виртуальной инфраструктуры, распределенные филиалы, мобильные сотрудники и домашние офисы, фрагментировали традиционный периметр и нарушили традиционную модель безопасности размещения решения NGFW на границе сети для наблюдения за движением трафика. и вперед через границу. Каждая новая сетевая среда теперь связана со своими уникальными требованиями и проблемами, и в результате решения безопасности начали

появляться как грибы по всей сети. Это создало уровень сложности с точки зрения развертывания, оптимизации и управления, который перегрузил большинство ИТ-команд. Это проблема, которую традиционный подход к платформе безопасности не может решить.

Согласно недавнему опросу IBM, на предприятии в настоящее время развернуто в среднем 45 инструментов безопасности. И что еще хуже, каждый инцидент, на который им нужно реагировать, требует координации с помощью 19 различных инструментов. К сожалению, эти инструменты изначально не предназначены для такого рода взаимодействия. Организации снова борются с разрастанием поставщиков и решений, вынуждены вручную сопоставлять аналитические данные об угрозах и ограничены в своей способности внедрять любые виды автоматизации для упрощения процесса. Это одна из причин, по которым время ожидания для нарушений безопасности теперь измеряется месяцами, и почему, по данным IBM, стоимость нарушения безопасности сейчас превышает 8,6 миллиона долларов за нарушение безопасности данных в США.

Потребность в новой платформе безопасности

Необходим новый подход к платформе безопасности. Тот, который объединяет все критически важные функции безопасности, необходимые организациям, в единое решение, которое может защитить всю сеть и позволить любому пользователю на любом устройстве безопасный доступ к любым данным или приложению, где бы оно ни находилось. Но чтобы заставить его работать в сегодняшних распределенных сетевых средах, нам нужно решить проблемы первой итерации этого подхода. А для того, чтобы это произошло, эффективная платформа безопасности должна быть построена на основе трех критических концепций: она должна быть широкой, интегрированной и автоматизированной.

Платформа, которую можно развернуть где угодно

Чтобы платформа безопасности была эффективной, ее необходимо последовательно и легко развертывать на каждом краю, будь то традиционные или распределенные центры обработки данных, общедоступные облачные среды или филиалы и торговые точки. А из-за роста количества устройств Интернета вещей, домашних офисов и мобильных пользователей вне сети его необходимо распространить и на эти места. Он должен работать в любой облачной среде, существовать во всех возможных форм-факторах и быть развернутым в любой среде.

Такой широкий подход гарантирует, что он может обеспечить одинаковую и последовательную защиту, будь то безопасность небольшого предприятия с небольшим количеством мест, сложной среды, такой как система здравоохранения с больницами, клиниками и кабинетами врачей, или высокоскоростной транзакционной среды, такой как торговый зал. или игровая среда, фармацевтическая или авиационная компания, использующая огромные потоки слонов для моделирования и трехмерного рендеринга, или крупная многонациональная компания с местоположениями, охватывающими несколько географических регионов.

Каждый компонент должен работать вместе

В отличие от платформ безопасности прошлого, эффективное решение должно включать инструменты, предназначенные для работы как единой интегрированной системы. Это означает, что решения безопасности, которые являются частью этой платформы, должны либо работать в общей операционной системе, либо использовать открытые API-интерфейсы, либо создаваться с использованием общих стандартов. Открытая система также означает, что можно использовать инструменты от разных поставщиков, сохраняя при этом возможность взаимодействия, что позволяет организациям использовать инструменты, которые были протестированы и утверждены, чтобы обеспечить наилучшее возможное решение.

В сегодняшних высокодинамичных средах интеграция должна выходить за рамки только элементов безопасности платформы. Безопасность и сеть также должны функционировать как единое решение, концепция, известная как сеть, управляемая безопасностью. Таким образом, когда сеть адаптируется к изменениям в среде, настраивая соединения или масштабируя ресурсы, безопасность может автоматически реагировать как часть полностью интегрированной системы.

И все это должно быть заключено в общую систему управления и оркестровки, предназначенную для расширения видимости и контроля во всей распределенной сети. Это включает корреляцию аналитических данных об угрозах, собранных с любого устройства безопасности в любом месте, централизацию конфигураций, обеспечение согласованного применения политик и координацию единого ответа на обнаруженные угрозы.

Платформа для поддержки автоматизации существует

Приступы могут произойти в мгновение ока. Учитывая изощренность и скорость сегодняшних атак, у защитников нет времени или ресурсов, чтобы сопоставить информацию об угрозах или рыться в горах файлов журналов из различных решений, чтобы обнаружить проблему. Это требует автоматизации. Но такая автоматизация невозможна, если решения безопасности предназначены для работы изолированно.

Когда инструменты могут работать как единое решение, такие вещи, как машинное обучение и искусственный интеллект, могут позволить организации обнаруживать, расследовать и реагировать на угрозы с цифровой скоростью. Даже передовые системы управления, от XDR до SIEM и SOAR для NOC и SOC, все улучшаются, когда отдельные устройства, которые они контролируют и которыми управляют, предназначены для совместной работы.

Современные сети требуют нового подхода к безопасности

Вызовы, с которыми сталкиваются организации сегодня, не могут быть решены с помощью тех же систем и стратегий, которые мы использовали раньше. Безопасность необходимо адаптировать так же полно, как и сети, которые они должны защищать. Платформа безопасности была хорошей идеей, когда она была представлена более двух десятилетий назад, и до сих пор остается отличной идеей. Однако концепцию необходимо адаптировать и обновлять, как и все остальное.

Сегодняшняя платформа безопасности должна охватывать всю сеть и адаптироваться по мере расширения и развития среды, которую она защищает. Для этого требуется платформа, спроектированная вокруг трех важнейших

компонентов широкого развертывания и внедрения, полной интеграции между элементами безопасности и сети, а также поддержки расширенной автоматизации, основанной на машинном обучении и ИИ». ***(John Maddison. The Growing Need for a New Security Platform // Wired Business Media (https://www.securityweek.com/growing-need-new-security-platform). 25.03.2021).***

***

«Panasonic Corporation и McAfee Corp. (Nasdaq: MCFE) договорились совместно начать строительство Центра управления безопасностью транспортных средств (далее именуемого SOC для транспортных средств) для коммерциализации систем безопасности транспортных средств. услуги мониторинга. Чтобы защитить подключенные к сети автомобили по всему миру от кибератак, компании создадут SOC для транспортных средств, которые позволят точно обнаруживать атаки и своевременно реагировать на них, а также помогут усилить меры кибербезопасности в автомобильной промышленности.

Panasonic уже использует SOC для заводов с 2016 года для защиты систем и сетей, которые управляют и контролируют заводское оборудование и производственные процессы от кибератак - до SOC для автомобилей. Для автомобилей они разработали автомобильную систему обнаружения вторжений, которая устанавливается на транспортном средстве, обнаруживает возникновение кибератаки и тип атаки и передает данные анализа в SOC транспортного средства и систему управления информацией и событиями безопасности, которая анализирует и визуализирует большой объем данных, полученных от автомобильной системы обнаружения вторжений в SOC транспортного средства. McAfee поддерживает SOC мирового класса и Managed Security Services (MSS), а также обладает ноу-хау, накопленным за счет создания и оперативной поддержки множества SOC.

С инновационным развитием автономного вождения, развитием цифровых технологий и увеличением количества подключенных автомобилей риск кибератак на автомобили возрастает с каждым годом. Для автомобильной промышленности стало срочно создавать механизмы защиты и мониторинга транспортных средств от кибератак. Центр управления безопасностью транспортных средств позволит предоставлять услуги по мониторингу подключенных автомобилей по всему миру и внесет свой вклад в развитие безопасного и безопасного общества мобильности». ***(Panasonic and McAfee Agree to Jointly Start Building Vehicle SOC for Commercialization of Vehicle Security Monitoring Services // Business Wire, Inc. (https://www.businesswire.com/news/home/20210329005701/en/Panasonic-and-McAfee-Agree-to-Jointly-Start-Building-Vehicle-SOC-for-Commercialization-of-Vehicle-Security-Monitoring-Services/). 30.03.2021).***

***

«Cloudflare выпустила новую функцию, которая направлена на защиту веб-сайтов от Magecart и других вредоносных атак на основе JavaScript.

Типичная кибератака - внедрение вредоносного JavaScript на веб-сайт для перенаправления посетителей на вредоносные сайты, отображения фишинговых

форм, использования уязвимостей и кражи предоставленной платежной информации.

Чтобы внедрить вредоносные сценарии на веб-сайт, злоумышленники обычно добавляют вредоносный встроенный JavaScript на веб-страницу, добавляют внешний вредоносный файл зависимостей JavaScript под свой контроль или компрометируют существующий сторонний сценарий в атаке цепочки поставок.

Когда JavaScript загружается из внешнего местоположения в качестве зависимости, во многих случаях они остаются незамеченными в течение длительного времени, особенно когда нет внешних изменений в пользовательском опыте сайта.

Например, атаки Magecart проводятся путем внедрения вредоносного кода JavaScript, который крадет информацию о кредитной карте, отправленную на веб-сайте. Поскольку эти данные незаметно передаются в удаленное место и покупки продолжаются, как обычно, пользователи не заметят ничего странного, о чем они должны сообщить сайту.

Из-за этого атаки Magecart могут незаметно красть кредитные карты у посетителей в течение многих месяцев, если не лет, прежде чем они будут обнаружены и устранены.

Page Shield для защиты от вредоносных скриптов

Сегодня Cloudflare анонсировала новую функцию безопасности под названием Page Shield, которая будет обнаруживать атаки в браузерах конечных пользователей, вызванные вредоносными зависимостями JavaScript.

«Наша миссия - помочь улучшить Интернет. Это распространяется на браузеры конечных пользователей, где мы наблюдаем тревожный рост атак за последние несколько лет. С помощью Page Shield мы поможем приложениям обнаруживать и смягчать эти неуловимые атаки, чтобы обеспечить безопасность конфиденциальной информации своих пользователей», - заявила сегодня Cloudflare.

С сегодняшним выпуском Page Shield Cloudflare начинает с инструмента Script Monitor, который будет сообщать Cloudflare каждый раз, когда посетитель на защищенном сайте запускает файл зависимостей JavaScript в своем браузере.

Используя эти отчеты, Cloudflare будет создавать историю известных скриптов, используемых на сайте. Обнаружив новый, сообщите об этом администратору веб-сайта, чтобы он мог продолжить расследование.

Используя Script Monitor, веб-администраторы могут обнаруживать подозрительные файлы JavaScript, загружаемые посетителями на их сайты, и быстро выяснять, являются ли они вредоносными.

Хотя это хорошее начало, это не защищает посетителей от существующих зависимостей JavaScript, которые были изменены в результате атаки на цепочку поставок.

Например, если сайт исторически загружал файл JavaScript с https://www.example.com/js/harmless.js и злоумышленник изменил этот файл на example.com, Script Monitor не обнаружит изменение, и вредоносный код будет разрешен для выполнения при атаке на цепочку поставок.

В будущем Cloudflare заявляет, что они планируют добавить дополнительные функции, которые будут выдавать предупреждения, когда содержимое сценария изменяется или содержит вредоносные сигнатуры.

В целом, это замечательный инструмент для пользователей Cloudflare, который помогает определить, был ли ваш сайт взломан для загрузки вредоносных файлов JavaScript.

Однако эта функция доступна только для подписок Business и Enterprise, и пользователи с уровнями Pro или Free не смогут воспользоваться этой услугой…». ***(Lawrence Abrams. Cloudflare Page Shield: Early warning system for malicious scripts // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/cloudflare-page-shield-early-warning-system-for-malicious-scripts/). 25.03.2021).***

***

«МегаФон первым среди операторов связи запустил многофункциональное решение «Платформа кибербразведки». Платформа создана для предиктивной работы с киберугрозами и позволит банкам предотвращать кражу денег со счетов клиентов, а корпоративному бизнесу – защитить своих сотрудников от мобильного мошенничества.

Платформа аккумулирует информацию обо всех современных источниках сетевых атак на пользователей мобильной связи. Разработанные МегаФоном алгоритмы в автоматическом режиме анализируют потоки сетевых событий и выявляют номера, которые находятся под угрозой хищения средств или информации. В частности, алгоритмы фиксируют распространение ссылок на вредоносное ПО, и по подозрительному характеру поведения пользователя платформа выявляет зараженные устройства, отслеживает обращение к фишинговым ресурсам.

«Автоматизированный сбор данных на платформе ускоряет их обработку сотрудниками служб информационной безопасности наших заказчиков. Это помогает клиентам МегаФона идентифицировать активность злоумышленников на ранних этапах и оперативно на нее реагировать. Мы рады предложить рынку новый взгляд на управление киберугрозами, связанными с мобильным мошенничеством», – говорит директор по развитию корпоративного бизнеса МегаФона Наталья Талдыкина.

Пользователь системы в личном кабинете «Платформы кибербразведки» получает оперативные отчеты по своему пулу номеров – своих сотрудников, пользователей корпоративной связи, или клиентов, давших согласие на получение информации о предупреждении мошенничества.

Информация обновляется по мере обнаружения новых угроз, поэтому компании могут оперативно связаться со своими клиентами или сотрудниками, предупредить их о потенциальной опасности. У банков при получении информации об угрозе в отношении клиента есть возможность приостановить подозрительную операцию и связаться с клиентом для дополнительного подтверждения.

«Благодаря аналитике больших данных платформа кибербразведки обнаруживает подозрительное использование услуг мобильной коммерции и

платежей, например, для вывода средств после хищений с применением социальной инженерии. Разработанные МегаФоном алгоритмы платформы позволяют определить конкретные мобильные кошельки и номера абонентов, вовлеченных в сомнительные финансовые операции. Банки получают сигнал о возможных подозрительных активностях и могут заблокировать транзакции», – говорит Сергей Хренов, директор по предотвращению мошенничества и потерь доходов МегаФона.

Пользователям платформы также доступен актуальный перечень выявленных фишинговых интернет-ресурсов, который регулярно пополняется и помогает в работе служб безопасности компаний.

Отдельный функционал платформы разработан для онлайн-сервисов и позволяет выявлять недобросовестных пользователей, которые используют сим-карты для массовой автоматизированной регистрации с целью мошеннических операций. Например, ритейл или сервисы каршеринга смогут выявлять «оптовых» пользователей бонусных баллов и скидок, социальные сети – бороться с созданием фейковых аккаунтов и накрутками. С таких аккаунтов также зачастую производится регистрация электронных кошельков, спам-рассылки по другим пользователям сервисов, мошенничества с использованием методов социальной инженерии на сайтах по размещению бесплатных объявлений». ***(МегаФон создал платформу киберразведки // ООО "ИКС-МЕДИА" (https://www.iksmedia.ru/news/5725842-MegaFon-sozdal-platformu-kiberrazve.html). 25.03.2021).***

***