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

№ 2 (лютий)

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.– №2 (лютий) . – 280 с.

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

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

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

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

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

ЗМІСТ

Стан кібербезпеки в Україні 5
Національна система кібербезпеки 6
Правове забезпечення кібербезпеки в Україні 8
Кібервійна проти України 8
Боротьба з кіберзлочинністю в Україні 13
Коронавірус COVID-19 та питання кібербезпеки 17
Світові тенденції в галузі кібербезпеки 23
Сполучені Штати Америки 40
Країни ЄС та Великобританія 48
Російська Федерація та країни ЄАЕС 60
Австралія 60
Інші країни 66
Протидія зовнішній кібернетичній агресії 76
Створення та функціонування кібервійськ 79
Кібератака на SolarWinds 79
Кіберзахист критичної інфраструктури 83
Захист персональних даних 87
Кіберзлочинність та кібертероризм 135
Діяльність хакерів та хакерські угруповування 172
Вірусне та інше шкідливе програмне забезпечення 186
Операції правоохоронних органів та судові справи проти кіберзлочинців 229
Технічні аспекти кібербезпеки 232
Виявлені вразливості технічних засобів та програмного забезпечення 232
Технічні та програмні рішення для протидії кібернетичним загрозам 264
Питання криптографії 280

«З 19 лютого у Кропивницькому працює консультаційний пункт з кібербезпеки. Про це Суспільному розповіла консультантка міського центру професійного розвитку педагогічних працівників Марина Сосновська. Завдання пункту – консультувати шкільних психологів та класних керівників вчити школярів протидіяти загрозам в інтернеті.

За словами Марини Сосновської, консультуватимуть на постійній основі. Групові консультації планують проводити раз на три місяці. Індивідуальні – за запитом.

”Збиратимемось, наприклад, на початку навчального року, на початку літа, коли діти залишатимуться без нагляду батьків. Це буде обов’язково. Інші консультації – відповідно до запиту. Допомагатимемо усім, хто цього потребуватиме”.

До роботи залучатимуть працівників патрульної поліції, ювенальної превенції та інших.

”Ми постійно над цим працюємо, робота велась до випадків отруєнням школярок на Київщині і Черкащині. Робота спрямована на необхідність поєднання суспільних зусиль на протидію та профілактику виникнення подібніх ситуацій".

До участі у першому семінарі, 19 лютого, запросили інспектора патрульної поліції Антона Левандовського». ***(Ірина Куніцька. У Кропивницькому працює консультаційний пункт з кібербезпеки // АТ «НСТУ» (https://suspilne.media/107918-u-svitlovodsku-likviduvali-upravlinna-osviti-ta-stvorili-nove/). 19.02.2021).***

***

«Блокування «Вконтакте», російської соціальної мережі, посприяло появі шкідливих додатків для браузерів для обходу блокування. Розширення VK Unblock для браузерів Chrome та Edge містило шкідливий код для викрадення даних з облікових записів Google.

Даний код таємно збирав дані користувачів та міг змінювати результати пошуку. Про це повідомили в Національному координаційному центрі кібербезпеки, який діє при Раді національної безпеки та оборони (РНБО).

Повідомляється, що такі шкідливі додатки встановили понад 3 млн користувачів, а основні країни, на які було спрямовано атаку, — Україна, Франція та Бразилія. Зараз ці шкідливі розширення заблоковані компаніями Google та Microsoft…» ***(На крадіжці даних підловили додаток для обходу блокування «ВКонтакте» // Ракурс (https://racurs.ua/ua/n150045-na-kradijci-danyh-pidlovyly-dodatok-dlya-obhodu-blokuvannya-vkontakte.html). 06.02.2021).***

***

«Кабінет Міністрів України на сьогоднішньому засіданні ухвалив постанову, яка передбачає створення національного центру резервування державних інформаційних ресурсів.

Влітку 2020 року Мінцифра розпочала активну фазу реформи кібербезпеки, яка передбачає, поміж іншого, розвиток ефективного і сучасного національного кіберцентру, а також заміну сертифіката безпеки КСЗІ Держспецзв'язку та інших застарілих стандартів безпеки 90-х. На їх місці мають з'явитися сучасні рішення, які забезпечать належний захист державної ІТ-інфраструктури та реєстрів.

Наприкінці минулого року Мінцифра та Держспецзв'язку взялись за впровадження системи моніторингу кіберінцидентів, яка фактично стала першим кроком в рамках реформи кібербезпеки.

В рамках прийнятого сьогодні рішення уряд врегулював механізм зберігання державних даних. Його невіддільною частиною стане так зване сховище для резервного зберігання всіх документів, даних державного значення. У разі видалення або пошкодження даних в результаті збою у системі з резервного сховища можна буде відновити все необхідне. Зокрема там будуть зберігатись дані державних реєстрів, бази даних органів влади та їх інформаційно-аналітичні системи, які пов'язані з наданням послуг громадянам. Відповідальним за роботу резервного сховища буде національний центр резервування державних інформаційних ресурсів.

Національний центр займатиметься:

забезпеченням безперервності роботи державних інформаційних ресурсів, резервного копіювання інформації;

забезпеченням надійного функціонування серверів, системи зберігання даних та контролю за статистичними даними роботи фізичного захисту об'єктів, системи управління та моніторингу.

Постанови розроблені відповідно до Стратегії кібербезпеки України, одним з основних пріоритетних завдань якої є кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури». ***(Владимир Скрипин. Реформа кібербезпеки: Кабмін схвалив створення національного центру резервування державних інформаційних ресурсів // ООО «ХОТЛАЙН» (https://itc.ua/news/reforma-kiberbezpeki-kabmin-shvaliv-stvorennya-naczionalnogo-czentru-rezervuvannya-derzhavnih-informaczijnih-resursiv/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+itc-ua+%28ITC.ua%29). 09.02.2021).***

***

«Президент Володимир Зеленський збільшив чисельність працівників Ради нацбезпеки та оборони, а також затвердив структуру РНБОУ. Відповідний указ, датований 26 лютого, опублікували на сайті Офісу голови держави.

"Відповідно до пункту 18 частини першої статті 106 Конституції України та Закону України "Про Раду національної безпеки і оборони України" постановляю

затвердити граничну чисельність працівників Апарату Ради національної безпеки і оборони України у кількості 237 штатних одиниць", - йдеться в указі №76/2021.

Крім того, указ передбачає затвердження наступної структури РНБОУ:

Секретар Ради національної безпеки і оборони України

перші заступники Секретаря Ради національної безпеки і оборони України

заступники Секретаря Ради національної безпеки і оборони України

Керівник Апарату Ради національної безпеки і оборони України

перший заступник та заступники Керівника Апарату Ради національної безпеки і оборони України

головний державний аудитор

Служба з питань запобігання та виявлення корупції

Служба Секретаря Ради національної безпеки і оборони України

Служба з питань зовнішньої безпеки

Служба з питань інформаційної безпеки та кібербезпеки

Служба з питань державної та громадської безпеки

Служба з питань воєнної безпеки

Служба з питань мобілізації та територіальної оборони

Служба з питань військово-технічного співробітництва та оборонно-промислового комплексу

Служба з питань економічної безпеки

Служба з питань соціальної та гуманітарної безпеки

Служба з питань безпеки критичної інфраструктури

Служба з питань зовнішньополітичної безпеки та міжнародного співробітництва

Служба з питань фінансового забезпечення виконання заходів у сфері національної безпеки і оборони

Служба з питань інформаційних технологій

Служба Головного ситуаційного центру

Служба організаційного забезпечення

Служба з питань стратегічного планування та аналізу

Служба забезпечення доступу до публічної інформації та зв'язків із засобами масової інформації

Служба з правових питань

Фінансова служба

Служба управління персоналом

Служба режимно-секретної роботи

Служба координаційної та адміністративної роботи…» ***(Зеленський збільшив чисельність працівників апарату РНБОУ та затвердив її склад // Дзеркало тижня. Україна (https://zn.ua/ukr/POLITICS/zelenskij-zbilshiv-chiselnist-pratsivnikiv-rnbo-ta-zatverdiv-jiji-sklad.html). 26.02.2021).***

***

«Сегодня Правительством приняты изменения в Правила обеспечения защиты информации в информационных, телекоммуникационных и информационно-телекоммуникационных системах, наработанные рабочей группой в составе специалистов Госспецсвязи, Минцифры, Гостаможслужбы и экспертов отрасли.

Принятие этого постановления позволит в полной мере использовать современные сетевые технологии и обеспечивать качественное внедрение электронных сервисов взаимодействия между органами государственной власти.

Кроме того, данное решение обеспечивает гармонизацию актов Правительства в соответствие с требованиями действующего законодательства в сфере защиты информации, как:

-с Законами Украины «О защите информации в информационно-телекоммуникационных системах» и «О лицензировании видов хозяйственной деятельности»;

-требованиями к подключению систем, в которых обрабатывается служебная информация и информация, составляющая государственную тайну, к глобальным сетям передачи;

-криптографической защиты конфиденциальной информации в органах государственной власти, воинских формированиях, органах местного самоуправления, на предприятиях, в учреждениях и организациях, которые принадлежат к сфере их управления.

Также Администрация Госспецсвязи в трехмесячный срок разработает требования к средствам криптографической защиты информации в государственных органах». ***(Дмитрий Сизов. Сегодня кабмином принято постановление по защите информации // InternetUA (http://internetua.com/segodnya-kabminom-prinyato-postanovlenie-po-zasxite-informacii). 08.02.2021).***

***

Кібервійна проти України

«Українські ресурси сектора безпеки і оборони зазнають DDoS-атак з IP-адрес, які належать російським мережам обміну трафіком. Про це повідомила Рада національної безпеки і оборони.

"Починаючи з 18 лютого цього року, Національний координаційний центр кібербезпеки при РНБО України фіксує масовані DDoS-атаки на український сегмент інтернет, переважно на вебсайти сектора безпеки і оборони. Зокрема атаки здійснювалися на сайти Служби безпеки України, Ради національної безпеки і оборони України, ресурси інших державних установ та стратегічних підприємств. Встановлено, що джерелом цих скоординованих атак були IP-адреси, які належать певним російським мережам обміну трафіком", – йдеться в повідомленні.

В РНБО зазначили, що зловмисники використовують новий механізм кібератак, який не спостерігався раніше під час подібних інцидентів.

"Під час атаки вразливі веб-сервери державних органів інфікуються вірусом, який приховано робить їх елементом бот-мережі, що використовується для DDOS-атак на інші ресурси. При цьому системи безпеки інтернет-провайдерів визначають скомпрометовані веб-сервери як джерело атак та починають блокувати їхню роботу шляхом автоматичного внесення до "чорних списків". Таким чином, навіть після закінчення фази DDoS атаковані веб-сайти залишаються недоступними для користувачів", – пояснили в РНБО.

В Нацраді додали, що фахівці Національного координаційного центру кібербезпеки надають консультації та технічну допомогу для виявлення та реагування на цей вид кібератаки і пропонують одразу повідомляти НКЦК у разі виявлення компрометації сайтів чи DDoS-атак на адресу report@ncscc.gov.ua...» ***(РНБО повідомила про російські кібератаки на українські сайти сектора безпеки та оборони // 5 канал (https://www.5.ua/nauka/rnbo-povidomyla-pro-rosiiski-kiberataky-na-ukrainski-saity-sektora-bezpeky-ta-oborony-237544.html). 22.02.2021).***

***

«Національний координаційний центр кібербезпеки при Раді національної безпеки і оборони України повідомив про активне зростання фішингових атак з використанням теми вакцинації від COVID-19.

Як повідомляють у РНБО, на початку пандемії у світі щодня реєструвалося понад 18 мільйонів фішингових повідомлень, пов’язаних з темою COVID-19. З середини 2020 року їх кількість поступово зменшувалась, а фішингові атаки стали більш цілеспрямованими, а їх тематика постійно змінювалася — від доступності масок і тестів до розробки вакцин.

Наприкінці січня 2021 року центр кібербезпеки при РНБО виявив фішингову кібератаку, яка експлуатувала популярну серед українців тему про початок вакцинації від COVID-19 в країні. Невідомі зловмисники створили на популярній хостинговій платформі фейкову вебсторінку, яка імітувала сайт Міністерства охорони здоров’я України. Для розміщення сторінки нападники зареєстрували кілька доменів, які нагадували офіційний домен МОЗ України — moz.gov.ua. На цій фейковій сторінці було розміщено інформацію щодо початку з 25 січня обов’язкової вакцинації від COVID-19 із пропозицією завантажити файл (документ Word) із подробицями.

Документ, ясна річ, містив шкідливий код (макрос), який при відкритті файлу приховано від користувача завантажує та виконує інший шкідливий скрипт, який вже забезпечує віддалене управління зараженим комп’ютером. Після відкриття файлу нападники отримували повний доступ до комп’ютерів жертв.

Національний координаційний центр кібербезпеки спільно з CSIRT-NBU та CERT-UA проаналізував усі етапи розвитку атаки та заблокував фішингові домени, а також додатково проінформував всі організації, на які було спрямовано атаку. Фейкові домени мали такі імена: moz-gov-ua[.]com, moz-govua[.]com та mozgovua[.]com…». ***(Владимир Скрипин. РНБО попередив українців про***

зростання фішингових атак з використанням теми вакцинації від COVID-19 // ООО «ХОТЛАЙН» (https://itc.ua/news/rnbo-poperediv-ukra%d1%97nczіv-pro-zrostannya-fishingovih-atak-z-vikoristannyam-temi-vakczinaczi%d1%97-vid-covid-19/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+itc-ua+%28ITC.ua%29). 12.02.2021).

***

«З 27 січня по 2 лютого система захищеного доступу державних органів до мережі Інтернет заблокувала 6 DDoS-атак та 43,6 тис. різних видів атак. Про це повідомляє УНН із посиланням на пресслужбу Державної служби спеціального зв'язку та захисту інформації України.

Цитата

"Система захищеного доступу державних органів до мережі Інтернет заблокувала 43 671 різних видів атак, що на 9% менше, ніж попереднього тижня. Переважна більшість - це мережеві атаки прикладного рівня (97%). Також зафіксовано і заблоковано 6 DDoS-атак", - йдеться у повідомленні.

Деталі

Система кіберзахисту державних інформаційних ресурсів та об'єктів критичної інфраструктури на об'єктах моніторингу зафіксувала 3,1 млн підозрілих подій, що на 31% менше, ніж попереднього тижня. Переважна більшість зафіксованих підозрілих подій стосується спроб викрадення інформації (29%), спроб отримання прав адміністратора (29%), мережевого сканування (22%) та підозрілого виконувального коду (8%).

Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 3 705 кіберінцидентів, що на 9% більше, ніж попереднього тижня.

"Переважна більшість опрацьованих інцидентів належить доменній зоні UACOM (близько 99%). Основна кількість інцидентів стосується розповсюдження ШПЗ (90%) та фішингу (9%)", - вказано у повідомленні.

Доповнення

Голова Національної поліції України Ігор Клименко заявив, що в Україні минулого року було зареєстровано понад 5 тис. кіберзлочинів, в яких вдалося оперативно затримати 106 фігурантів кримінальних проваджень.

Зокрема, на ЦВК за рік було здійснено понад 1,8 млн кібератак». ***(Дар'я Панченко. За тиждень в Україні зафіксовано близько 44 тис. Кібератак // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1914913-za-tizhden-v-ukrayini-zafiksovano-blizko-44-tis-kiberatak). 02.02.2021).***

***

«На сайте CyberNews, который публикует новости о кибербезопасности, появилась статья о том, что в онлайне якобы продается база из 40 млн пользователей «ПриватБанка».

Что пишут о базе

Якобы базу банка продает на одном из хакерских форумов анонимное лицо, и в ней содержатся полные ФИО, дата рождения, налоговый номер, данные паспорта, семейное положение, мобильный номер, наличие авто и т.д…

Автор публикации просил за базу $3400 в биткоинах. На 12 февраля 2021 года по данным указанного биткоин-кошелька базу пока никто не купил, отмечает издание. Однако также возможно, что для каждой продажи анонимный автор генерирует новый кошелек.

Что говорят в банке

На запрос AIN.UA в банке ответили, что служба безопасности «ПриватБанка» не подтверждает информацию о появлении хакерского ресурса, якобы продающего персональные данные украинцев.

«В ходе исследования деятельности этого ресурса выяснилось, что он создан мошенниками, не имеющими и никогда не имевшими доступа к персональным данным какого либо из украинских банков и учреждений. Мошенники используют общедоступные объединенные ресурсы и выдают это за якобы имеющуюся «секретную» базу данных», — сообщили в банке.

По данным службы безопасности банка, с 2017 года она не зафиксировала ни одного случая копирования или передачи персональных данных из базы клиентов.

В банке также отметили, что к числу клиентов банка приписали 40 млн человек, при том, что эта цифра превышает количество совершеннолетнего населения Украины. Количество клиентов «ПриватБанка» — около 20 млн.

По данным одного из собеседников AIN.UA, возможно речь идет о продаже старых, ранее утекших в сеть баз данных, а слова «ПриватБанк» и «база 40 млн украинцев» используется для создания большего эффекта. Еще один собеседник AIN.UA из сферы киберзащиты указал, что впервые сталкивается с изданием CyberNews и не может подтвердить его авторитетность». ***(Ольга Карпенко. СМИ: Базу 40 млн пользователей «ПриватБанк» продают онлайн. В банке говорят, что база — не его // ain.ua (https://ain.ua/2021/02/15/sliv-dannyx-40-mln-polzovateley/). 15.02.2021).***

***

«Концерн "Центр коммунального сервиса" (ЦКС) снял с себя ответственность за возможные утечки информации из мобильного приложения "Коммуналка".

Напомним, ранее эксперты по кибербезопасности нашли в приложении критические изъяны.

В ответ на запрос UBR.ua в ЦКС отметили, что все зарегистрированные в приложении пользователи берут на себя ряд обязательств. Например, соглашение предусматривает ограничение по использованию персональных данных третьих лиц.

В частности, не использовать "Коммуналку" для:

сбора, хранения и обработки персональных данных других пользователей;

выдачи себя за другое лицо или представителя предприятия, учреждения или организации без достаточных для этого прав;

введения в заблуждение касательно характеристик любых субъектов и объектов.

«Следовательно, пользователь, который зарегистрировался в системе, должен осознавать ответственность за использование данных, размещенных в приложении», – подчеркнул первый заместитель генерального директора коммунального концерна ЦКС Вячеслав Олийнык.

Вместе с этим он отметил, что разработчик «Коммуналки» уже начал внедрение дополнительных мер по защите персональных данных». ***(Мыкола Олиярнык. Киев возложил ответственность за утечку данных из "Коммуналки" на самих пользователей // UBR.ua (https://ubr.ua/ukraine-and-world/technology/kiev-vozlozhil-otvetstvennost-za-utechku-dannykh-iz-komunalki-na-samikh-polzovatelej-3900306). 17.02.2021).***

***

«На головну сторінку порталу КМДА здійснювалася DDoS-атака.

Про це повідомив мер Києва Віталій Кличко.

“Друзі! На головну сторінку порталу КМДА відбувається DDoS-атака. За словами технічних спеціалістів, системи захисту налаштовані й відпрацьовують навантаження. Вибачаємося за тимчасові незручності, що можуть виникнути”, – написав він.

Кличко зазначив, що фахівці відновили роботу сайту.

Наразі з переглядом сторінок сайту kyivcity.gov.ua очевидних проблем немає.

На сайті з’явилося повідомлення про “можливі перебої” і прохання користуватися альтернативними джерелами інформації від КМДА, зокрема у соцмережах». ***(Хакери атакували портал КМДА // Букви (https://bykvu.com/ua/bukvy/hakeri-atakuvali-portal-kmda/). 10.02.2021).***

***

«В Україні у період з 3 по 9 лютого на 19% зросла кількість хакерських атак…

Цитата:

"Система захищеного доступу державних органів до мережі Інтернет заблокувала 53 766 різних видів атак, що на 19 % більше, ніж попереднього тижня. Переважна більшість - це мережеві атаки прикладного рівня (98%). Також зафіксовано і заблоковано 2 DDoS-атаки", - йдеться в повідомленні пресслужби.

Деталі

Система кіберзахисту державних інформаційних ресурсів та об’єктів критичної інфраструктури на об’єктах моніторингу зафіксувала 3 860 199 підозрілих подій, що на 22% більше, ніж попереднього тижня. Переважна більшість зафіксованих підозрілих подій стосується спроб отримання прав адміністратора (24%), спроб викрадення інформації (21%), мережевого сканування (20%) спроб отримання прав користувача (18%) та підозрілого виконувального коду (10%).

Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA у цей період зареєструвала та опрацювала 4 800 кіберінцидентів, що на 23% більше, ніж попереднього тижня.

Переважна більшість опрацьованих інцидентів належить доменній зоні UACOM (близько 99%). Основна кількість інцидентів стосується розповсюдження ШПЗ (64%) та фішингу (35%)…». ***(Дар'я Панченко. В Україні за тиждень на близько 20% зросла кількість хакерських атак // Інформаційне агентство «Українські Національні Новини» (https://www.unn.com.ua/uk/news/1915827-v-ukrayini-za-tizhden-na-blizko-20-zrosla-kilkist-khakerskikh-atak). 09.02.2021).***

***

«Національний координаційний центр кібербезпеки» при «Раді національної безпеки і оборони України» зафіксував спроби поширення шкідливих документів через «Систему електронної взаємодії органів виконавчої влади» (СЕВ ОВВ).

Метою атаки було масове зараження інформаційних ресурсів державних органів, оскільки саме з використанням цієї системи здійснюється документообіг у більшості органів державної влади.

Шкідливі документи містили макрос, який під час відкриття файлів приховано завантажував програму для віддаленого управління комп'ютером. Способи та засоби реалізації цієї кібератаки дозволяють пов'язати її з одним із хакерських шпигунських угруповань з Російської Федерації.

За сценарієм атака належить до так званих supply chain attack. Це атака на ланцюжок поставок, під час якої атакуючі намагаються отримати доступ до цільової організації не напряму, а через вразливості в інструментах і сервісах, які вона використовує…». ***(Хакери атакують систему документообігу державних органів // Компьютерное Обозрение (https://ko.com.ua/hakeri_atakuyut_sistemu_dokumentoobigu_derzhavnih_organiv_136447). 25.02.2021).***

***

Боротьба з кіберзлочинністю в Україні

«Павлоградский горрайонный суд Днепропетровской области приговорил к штрафу украинца за распространение вредоносного программного обеспечения…

Во время судебного заседания стало известно, что в июле 2019 года у жителя Павлограда возник преступный умысел на сбыт вредоносного программного обеспечения, предназначенного для несанкционированного вмешательства в работу компьютерных сетей. Для этого мужчина опубликовал в сети Интернет объявление, на которое в сентябре 2019 года откликнулся житель Днепра, с которым преступник договорился о сбыте устройства BlueWay BT-N9100 и программного обеспечения к нему, предназначенного для взлома wi-fi сетей. После получения оплаты в размере 420 гривен на банковскую карточку «Приватбанка», мужчина отправил вышеуказанное устройство заказчику в одно из отделений «Новой Почты» в г. Днепр.

Действия подсудимого были квалифицированы по ч. 1 ст. 361-1 УК Украины, как сбыт вредоносного программного обеспечения, предназначенного для несанкционированного вмешательства в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи.

На основании ст. 65 УК Украины, учитывая тяжесть преступления, личность обвиняемого, а именно то, что обвиняемый совершил нетяжкое преступление, ранее не судим, признал свою вину полностью, в содеянном раскаялся, суд посчитал, что наказание обвиняемому следует назначить в виде штрафа в размере 500 необлагаемых минимумов доходов граждан,что составляет 8500 гривен.

Также подсудимый должен оплатить сумму 6671 грн. 70 коп в счет возмещения процессуальных издержек». ***(Артем Сереженок. Суд приговорил украинца к штрафу за продажу вредоносного ПО // InternetUA (http://internetua.com/sud-prigovoril-ukrainca-k-shtrafu-za-prodaju-vredonosnogo-po). 18.02.2021).***

***

«Сообщается, что совместная операция правоохранительных органов Франции и Украины привела к аресту нескольких участников операции по вымогательству Egregor в Украине.

Как сначала сообщал France Inter, во вторник правоохранительные органы произвели аресты после того, как французские власти смогли отследить выплаты выкупа лицам, находящимся в Украине.

Считается, что арестованные являются филиалами Egregor, чьей задачей было взломать корпоративные сети и развернуть программы-вымогатели. France Inter также сообщает, что некоторые люди оказали материально-техническую и финансовую поддержку.

За последний год Egregor атаковал множество французских организаций, включая Ubisoft, Ouest France и, в последнее время, Gefko.

Об операции стало известно в ходе расследования, начатого прошлой осенью Высшим судом Парижа после получения жалоб на банду вымогателей.

В настоящее время сайты Tor компании Egregor отключены, в том числе сайт платежей и сайт утечки данных. Поскольку сайт оплаты Tor недоступен, жертвы не могут связаться с бандой вымогателей, заплатить выкуп или загрузить дешифраторы для ранее оплаченных выкупов.

Неизвестно, связаны ли проблемы с инфраструктурой банды вымогателей с операцией правоохранительных органов.

BleepingComputer.com связался с французскими правоохранительными органами, но не получил ответа.

Взлет и падение Эгрегора

Egregor работает как программа-вымогатель как услуга (RaaS), где аффилированные лица вступают в партнерские отношения с разработчиками программ-вымогателей для проведения атак и разделения выкупа.

В таких партнерствах разработчики программ-вымогателей несут ответственность за разработку вредоносного ПО и работу сайта платежей. В то же

время филиалы несут ответственность за взлом сетей жертв и развертывание программ-вымогателей.

В рамках этой договоренности разработчики зарабатывают от 20 до 30% от суммы выкупа, а остальные 70-80% вносят аффилированные лица.

Egregor запустился в середине сентября, когда одна из крупнейших групп, известная как Maze, начала сворачивать свою деятельность.

В то время злоумышленники сообщили BleepingComputer, что филиалы Maze перешли на Egregor RaaS, что позволило запустить новую операцию вымогателей с помощью опытных и квалифицированных хакеров.

В ноябре банда вымогателей объединилась с вредоносным ПО Qbot, чтобы получить доступ к сетям жертв, что еще больше увеличило объем атак.

Из-за того, что Egregor так быстро рос за относительно короткий период, жертвам приходилось стоять в очереди, чтобы договориться о платеже с помощью программы-вымогателя.

В начале декабря Эгрегор внезапно начал замедляться, и в ходе операции было проведено гораздо меньше атак. Вы можете увидеть это резкое снижение, начиная с 9 декабря 2020 года, на графике ниже, представленной Egregor для ID Ransomware.

В прошлом месяце Билл Сигел, генеральный директор компании Coveware, занимающейся переговорами о выкупе, сказал BleepingComputer, что они тоже заметили снижение количества атак Egregor, и сообщил нам, что филиалы могли перейти на другой RaaS.

В январе сайт утечки данных Эгрегора отключился примерно на две недели, а когда он снова заработал, возникли проблемы с сайтом. Это необычное действие заставило других злоумышленников заподозрить, что Эгрегор был взломан или взломан правоохранительными органами.

В настоящее время неизвестно, связано ли снижение активности Egregor с правоохранительными органами или просто с приливами и отливами операций с программами-вымогателями.

В новом отчете, опубликованном на прошлой неделе фирмой Kivu, занимающейся кибербезопасностью, исследователи заявляют, что с момента запуска Egregor накопил более 200 жертв и состоит из 10–12 основных участников и 20–25 частично прошедших проверку участников.

Некоторые из известных компаний, подвергшихся атаке со стороны Эгрегора, включают Barnes and Noble, Kmart, Cencosud, Randstad, систему метро TransLink Ванкувера и Crytek». ***(Lawrence Abrams. Egregor ransomware affiliates arrested by Ukrainian, French police // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/egregor-ransomware-affiliates-arrested-by-ukrainian-french-police/). 14.02.2021).***

***

«Фігурант спеціалізувався на розробці фішингових пакетів та адміністративних панелей для їхнього управління. Фішингові атаки були націлені на фінансові установи та злам поштових сервісів. У результаті

фішингових атак постраждали фінустанови 11 країн світу. За попередніми даними, збитки сягають десятків мільйонів доларів.

Зловмисника викрили працівники Департаменту кіберполіції спільно з Головним слідчим управлінням Нацполіції, Офісом Генерального прокурора України, в ході міжнародної спецоперації з правоохоронцями Сполучених Штатів Америки та Австралії.

Встановлено, що 39-річний житель Тернопільщини розробив фішинговий пакет і спеціальну адміністративну панель до нього, які були націлені на вебресурси банків та їх клієнтів. Адмінпанель дозволяє контролювати облікові записи користувачів, які зареєструвалися на скомпрометованих ресурсах та вводили свої платіжні дані. В подальшому ці дані отримували зловмисники.

Кожна фішингова атака була націлена на конкретну фінансову установу. Встановлено, що від фішингових атак постраждали фінансові установи Австралії, Іспанії, США, Італії, Чілі, Нідерландів, Мексики, Франції, Швейцарії, Німеччини та Великобританії.

За попередніми підрахунками, збитки від протиправної діяльності сягають десятків мільйонів доларів. За результатами аналізу іноземних правоохоронців, понад 50% усіх фішингових атак у 2019 році в Австралії було здійснено саме завдяки розробці фігуранта.

Хакер також розроблював фішингові ресурси, орієнтовані на злам поштових служб, які використовує понад 1,5 мільярда користувачів.

Для демонстрації функціоналу та продажу своїх розробок фігурант створив власний інтернет-магазин у Dark net.

Правоохоронці провели п’ять санкціонованих обшуків на території Тернопільської області. За результатами вилучено комп’ютерну техніку, мобільні телефони та жорсткі диски.

Під час огляду вилученої комп’ютерної техніки встановлено більше 200 активних покупців шкідливого програмного забезпечення. Хакер не лише збував свою продукцію клієнтам з усього світу, а й надавав технічну підтримку під час здійснення фішингових атак.

Відкрито кримінальне провадження за ч. 2 ст. 361 (Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) та 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. Санкція статті передбачає до шести років позбавлення волі. Слідчі дії тривають». ***(Кіберполіція припинила діяльність одного з найбільших у світі фішингових сервісів для атак на фінансові установи різних країн // Департамент кіберполіції Національної поліції України (https://cyberpolice.gov.ua/news/kiberpolicziya-prypynyla-diyalnist-odnogo-z-najbilshyx-u-sviti-fishyngovyx-servisiv-dlya-atak-na-finansovi-ustanovy-riznyx-krayin-506/). 04.02.2021).***

***

«Кіберфахівці СБУ викрили та припинили діяльність хакера, причетного до здійснення кібератак через бот-мережу на державні електронні інформаційні ресурси…

Зокрема, як зазначається в повідомленні, на початку цього року оперативники СБУ локалізували спробу хакерської атаки на автоматизовані системи держорганів Житомирщини. Зловмисники планували отримати віддалений доступ до комп'ютерів для зняття інформації, яка підлягає захисту. Вони також збирались уразити ПК шкідливим програмним забезпеченням, а потім приховано використовувати ресурси у бот-мережі для організації подібних кібератак.

У ході досудового розслідування слідчі СБУ задокументували, що для протиправної діяльності зловмисники використовували закордонні ресурси хостинг-провайдера із Львівщини. Додаткова перевірка підтвердила, що сервери розміщено на території Російської Федерації і належать фігуранту справи.

У ході санкціонованих обшуків за місцем проживання провайдера правоохоронці вилучили комп'ютерну техніку, яку передано для проведення відповідних досліджень.

Слідчі органів безпеки здійснюють досудове розслідування за ч. 1 ст. 111 (державна зрада) та ч. 2 ст. 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) Кримінального кодексу України. Перевіряється також інформація щодо можливої співпраці підозрюваного з представниками спецслужб країни-агресора.

Документування діяльності зловмисника здійснювали співробітники Управління СБУ в Житомирській області під процесуальним керівництвом Житомирської обласної прокуратури». ***(СБУ заблокувала ботмережу для російських кібератак на системи держорганів // iPress (https://ipress.ua/news/sbu_zablokuvala_botmerezhu_dlya_rosiyskyh_kiberatak_na_systemy_derzhorganiv_319626.html). 26.02.2021).***

***

Коронавірус COVID-19 та питання кібербезпеки

«Кибербезопасность заняла свое место в центре внимания организаций, обеспокоенных рисками во время пандемии COVID-19. Удаленная работа, набор коммуникационных решений и оборудования, используемых организациями, и ускоренное использование облачных аутсорсинговых решений увеличили цепочку потенциальных уязвимостей для кибератак.

РИСКИ КИБЕРБЕЗОПАСНОСТИ

Пандемия увеличила риск того, что киберпреступники проникнут к удаленному рабочему столу и получат доступ администратора, украдут и / или зашифруют конфиденциальную и конфиденциальную информацию и вымогают платежи за возврат этой информации. Распределенная атака отказа в обслуживании на Новозеландской фондовой бирже в августе 2020 года, лишившая ее

возможности публиковать публичные объявления и нарушившая торговую деятельность, как сообщается, была частью попытки вымогательства.

Поддельные учетные записи электронной почты, выдающие себя за знакомые контакты сотрудников, с целью получения конфиденциальной информации или передачи платежей являются особой проблемой. Множество методов связи и платформ виртуальных встреч, используемых сотрудниками, подрядчиками и поставщиками услуг на устройствах, могут скрывать признаки злонамеренного взаимодействия.

Многие организации ускорили переход на облачные решения в течение 2020 года, а безопасность интерфейса прикладного программирования (API) и риски неправильной настройки масштаба - другие ключевые проблемы, возникшие в прошлом году.

УПРАВЛЕНИЕ РИСКАМИ

Ниже обсуждаются соображения по снижению рисков кибербезопасности во время пандемии.

Усердие

При привлечении потенциальных ИТ-поставщиков или проверке текущих поставщиков, в дополнение к средствам контроля безопасности, которые ваша организация требует в «нормальное» время, определите средства контроля, необходимые для удаленных рабочих сред. Они могут относиться к

потоки данных и централизованное хранение данных;

методы удаленного доступа к сети вашей организации, включая средства контроля доступа, например, через фирменное оборудование или онлайн-порталы с использованием личного оборудования;

инвентарь устройств; и

использование субподрядчиков и прозрачность их политик и процедур обеспечения безопасности и доступа.

Управление доступом

Растущее число киберугроз, которые по-прежнему зависят от проникновения через пользователей конечных точек, является напоминанием о том, что в соглашениях об ИТ-услугах следует определять, кто такие авторизованные пользователи, и четко определять процессы утверждения, проверки и обновления для непрерывного доступа. Обязанности и контроль над привилегированными правами доступа должны быть надежными.

Для организации удаленной работы во время пандемии COVID-19 для некоторых организаций требовалось гибкое количество и состав пользователей системы, и в соглашениях следует учитывать это. Распределение ответственности за проверку пользователей и контроль доступа должно быть четко разграничено.

Гарантии

Организации могут требовать гарантий дополнительных уровней безопасности, принимаемых поставщиком для устранения рисков удаленной работы, таких как средства контроля за любой повышенной зависимостью от протокола удаленного рабочего стола, процедур доступа, физической безопасности домашних сред и связанных с этим рисков конфиденциальности. Другие более

общие гарантии могут подтверждать отсутствие вирусов и стандарты защиты от вирусов, установленные поставщиком.

Прозрачность

Обязательства по немедленному уведомлению поставщика о фактических и потенциальных нарушениях безопасности являются обычным требованием клиентов.

Чтобы справиться с повышенными рисками пандемии, организации могут требовать от поставщиков уведомлять и сообщать об обязательствах в отношении любых существенных сообщений о нарушениях данных, а не только о самих нарушениях, чтобы требовать прозрачности любых требований о вымогательстве или угроз утечки данных клиентов.

Хотя вышеперечисленные пункты не обеспечивают вакцины против всех рисков кибербезопасности, они могут предлагать договорные эквиваленты ношения лицевой маски и использования эффективной системы отслеживания и отслеживания для защиты ваших мер ИТ-безопасности, поскольку мы продолжаем действовать в этом новом обычном режиме». ***(PETER M. WATT-MORSE, JAMES MULLIGAN. Are Your IT Agreements COVID-19 Secure? // Morgan Lewis (https://www.morganlewis.com/blogs/sourcingatmorganlewis/2021/02/are-your-it-agreements-covid-19-secure-cv19-bp). 12.02.2021).***

***

«Кибератаки становятся все более привычной частью нашего ландшафта. Существование, основанное на данных, делает нас более уязвимыми, чем когда-либо прежде. К сожалению, в условиях пандемии COVID-19 сектор здравоохранения сталкивается с непропорционально высоким уровнем угрозы. Для того, чтобы новаторы в области кибербезопасности могли обеспечить безопасность своих технологий и эффективно выводить продукты на рынок, патентная защита является ключевым моментом. Тем не менее, хотя защита программных технологий может быть сложной задачей, это, безусловно, возможно, и диапазон того, что вы можете защитить, вполне может быть шире, чем вы думаете...

79% утечек данных происходят в сфере здравоохранения

Согласно отчетам Check Point и Fortified Health Security, организации, специализирующиеся на здравоохранении, составили 79% зарегистрированных утечек данных за первые десять месяцев 2020 года.

Это большая проблема. Определенные кибератаки могут быть разрушительными, например, заражение критически важных систем программами-вымогателями, которые могут замедлить их работу или сделать их неработоспособными, и атаки распределенного отказа в обслуживании (DDoS), которые перегружают сеть провайдера и внедряют вредоносное ПО в предположительно изолированные медицинские устройства, которые затем может заразить остальную часть сети (включая оборудование жизнеобеспечения).

Согласно этим отчетам, наиболее распространенным средством кибератак являются программы-вымогатели. Считается, что медицинские работники

особенно уязвимы, потому что любое нарушение их работоспособности опасно для жизни, что увеличивает вероятность их выплаты выкупа.

Тем не менее, хотя предотвращение атак программ-вымогателей является ключевым фактором, природа киберпреступности означает, что сосредоточение ресурсов только на одном типе атаки может подвергнуть те же системы другим формам киберпреступности. Может показаться драматичным сказать, что между поставщиками медицинских услуг и киберпреступниками развивается гонка вооружений, но там, где жизни угрожают, такое заявление кажется соразмерным.

Технологии кибербезопасности - что можно защитить патентами?

Если вы вводите новшества для разработки технологий, которые могут помочь предотвратить кибератаки на поставщиков медицинских услуг, вам следует рассмотреть возможность подачи патентных заявок для защиты базовой технической концепции.

Патенты защищают от третьих лиц, которые могут попытаться скопировать вашу технологию. Даже если вы применили ранее известные технологии для решения конкретной проблемы в области здравоохранения, у вас все равно может быть аргумент в пользу обеспечения патентной защиты ваших технических инноваций. Решения по кибербезопасности часто могут включать в себя сочетание аппаратного и программного обеспечения, требующего опытного и знающего подхода для обеспечения адекватной защиты.

В нашу команду по программному обеспечению и технологиям входят консультанты с обширным опытом защиты технологий в сфере здравоохранения, особенно тех, которые обеспечивают улучшенную кибербезопасность в технических архитектурах. Это дает нам уникальный взгляд на то, как могут проявляться киберугрозы». ***(DR TERENCE BRODERICK. The healthcare cybersecurity arms race — is your IP protected? // URQUHART-DYKES & LORD LLP (https://www.udl.co.uk/insights/the-healthcare-cybersecurity-arms-race-is-your-ip-protected). 08.02.2021).***

***

«Исследователи разработали инструмент для выявления рисков безопасности и конфиденциальности, связанных с приложениями для отслеживания контактов Covid-19.

COVIDGuardian, первый автоматизированный инструмент оценки безопасности и конфиденциальности, тестирует приложения для отслеживания контактов на предмет потенциальных угроз, таких как вредоносное ПО, встроенные средства отслеживания и утечка частной информации.

Используя инструмент COVIDGuardian, эксперты по кибербезопасности оценили 40 приложений для отслеживания контактов Covid-19, которые используются во всем мире, на предмет потенциальных угроз конфиденциальности и безопасности. Их выводы включают следующее:

72,5% приложений используют хотя бы один небезопасный криптографический алгоритм.

Три четверти приложений содержат по крайней мере один трекер, который передает информацию третьим лицам, таким как Facebook Analytics или Google Firebase.

Хотя в большинстве приложений не было вредоносных программ, в приложении для Кыргызстана Stop COVID-19 KG было обнаружено вредоносное ПО.

После своего анализа исследователи предоставили результаты поставщикам. Дальнейшее тестирование позже показало, что недостатки конфиденциальности и безопасности в четырех приложениях были исправлены, а одно уязвимое приложение больше не было доступно.

Доктор Гарет Тайсон, старший преподаватель Лондонского университета королевы Марии, сказал: «В связи с пандемией возникла острая необходимость в приложениях для отслеживания контактов для поддержки усилий по борьбе с распространением Covid-19. Неудивительно, что мы обнаружили, что это привело к относительно основные ошибки безопасности появляются во всем мире. Некоторые из наиболее распространенных рисков связаны с использованием устаревших криптографических алгоритмов и хранением конфиденциальной информации в текстовых форматах, которые могут быть прочитаны потенциальными злоумышленниками».

«Наша работа помогает разработчикам решать эти проблемы. С помощью COVIDGuardian мы создали инструмент, который могут использовать разработчики для обнаружения и исправления потенциальных недостатков в своих приложениях, а также для предоставления рекомендаций, которые помогут обеспечить конфиденциальность и безопасность пользователей».

Чтобы поддержать эту работу, исследователи также провели опрос, в котором приняли участие более 370 человек, чтобы понять вероятность того, что они будут использовать приложение для отслеживания контактов, и выявить проблемы, связанные с их использованием. Результаты показали, что конфиденциальность и точность приложений для отслеживания контактов оказали наибольшее влияние на то, будут ли люди использовать приложение.

В рамках опроса волонтеров также спросили об их предпочтениях в отношении децентрализованных и централизованных приложений. Д-р Тайсон сказал: «Проблемы безопасности и конфиденциальности были большой проблемой, повлиявшей на распространение этих приложений. Мы были удивлены, что дебаты вокруг децентрализованных и централизованных приложений не казались такими важными, и вместо этого пользователи были больше сосредоточены на точном подробности о том, какая личная информация собирается. Это должно побудить разработчиков предложить более строгие гарантии конфиденциальности для своих приложений». ***(New tool reveals security and privacy issues with contact tracing apps // Newswise (https://www.newswise.com/coronavirus/new-tool-reveals-security-and-privacy-issues-with-contact-tracing-apps/?article_id=746848). 25.02.2021).***

***

«…В отчете под названием «Оценка безопасности вакцины против COVID-19» аналитики G4S подробно описывают угрозы безопасности - как

физические, так и кибернетические, - связанные с распространением вакцины на территории США.

В отчете подробно описаны самые большие риски безопасности, связанные с распространением вакцин, в том числе:

Подделки

Помимо мошенничества, связанного с СИЗ, веб-сайтами, чистящими средствами, компаниями и услугами, связанными с COVID-19, в отчете говорится, что «риск подделок, вероятно, снизится в долгосрочной перспективе, если доступность законных вакцин будет соответствовать темпам спроса. ; однако, если дефицит будет продолжаться и более бедные страны не смогут получить достаточное количество вакцин, то, согласно оценкам безопасности и разведывательной информации G4S, риск подделок останется очень высоким».

Кража

В отчете делается вывод, что кража вакцин в США пока минимальна, но в среднесрочной перспективе может увеличиться по мере того, как нас расширяет распространение. «G4S оценивает, что крупномасштабные кражи представляют собой относительно низкий риск в США, но могут представлять больший риск в других странах, где доступ к вакцине по-прежнему ограничен, где преобладают организованная преступность и торговцы людьми и / или где есть более высокий уровень коррупции».

Саботаж

Согласно отчету, также существует риск единичных случаев саботажа вакцинации. Это особенно вероятно у людей, которые разделяют теории заговора против вакцины. Например, фармацевт Стивен Бранденбург признал себя виновным в попытке подделать вакцину Moderna на предприятии в Висконсине.

Кража PII

Аналитики G4S считают, что риск кражи личной идентифицируемой информации (PII) высок. «Процесс регистрации на прием по вакцинации - обычно через Интернет - предоставление личной идентифицируемой информации и ощущение срочности записи на прием могут увеличить шансы того, что люди не обратят внимания на признаки мошенничества».

Шпионаж

Аналитики разведки также считают, что общий риск шпионажа повышается во время путешествий - даже в дружественные страны. «Хранящиеся на телефоне данные человека об отслеживании вакцины, симптомах и т. Д. Могут стать привлекательной целью для спецслужб принимающей страны».

Информационная безопасность

Ландшафт киберугроз, связанный с безопасностью вакцины COVID-19, значительно расширился и теперь включает в себя финансируемые государством (т.е. «расширенные постоянные угрозы»), а также отдельные криминальные хакерские операции. Угрозы кибербезопасности значительны.

Дезинформация

По мнению аналитиков G4S, распространение дезинформации, дезинформации, обмана и мошенничества представляет собой высокий, устойчивый и долгосрочный риск для безопасности вакцин.

Протесты

В отчетах говорится, что риск протестов сохранится в течение 2021 года и, скорее всего, будет сосредоточен вокруг мест массовой вакцинации, правительственных зданий и корпоративных зданий производителей вакцин. «Организации и частные лица, фигурирующие в теориях заговора, связанных с COVID-19, также могут стать мишенью. Возможны единичные акты насилия, аналогичные тем видам изолированной деятельности, которые наблюдались в последние месяцы в отношении частных лиц или предприятий, пытающихся применить другие меры здравоохранения, такие как ношение масок».

Физическая охрана

Согласно отчету, существует риск отдельных атак на усилия по оказанию помощи в связи с COVID-19, например, на предприятиях по производству и отправке вакцин и, в частности, на объекты вакцинации, которые могут иметь мало возможностей для контроля доступа или повышения безопасности. «Этот риск оценивается как наиболее вероятный для отдельных лиц или небольших групп, которые придерживаются теорий заговора, и является крайне непредсказуемым, поскольку может возникнуть практически без предупреждения и в местном масштабе».

Согласно отчету, общий высокий риск мошенничества может повлиять на несколько угроз безопасности. Например, мошенничество и мошенничество распространяются посредством дезинформации и дезинформации, включают подделку и могут привести к краже личной идентифицируемой информации…» ***(COVID-19 vaccine security: an assessment of the risks, both physical and cyber // BNP Media (https://www.securitymagazine.com/articles/94704-covid-19-vaccine-security-an-assessment-of-the-risks-both-physical-and-cyber). 26.02.2021).***

***

Світові тенденції в галузі кібербезпеки

«На этой неделе центр кибербезопасности Proofpoint подал иск против Facebook в связи с попыткой социальной сети конфисковать доменные имена, которые охранная фирма использовала для обучения осведомленности о фишинге.

Дело представляет собой встречный иск к заявке Facebook от 30 ноября 2020 года, когда социальная сеть использовала запрос UDRP (Uniform Domain-Name Dispute-Resolution), чтобы заставить регистратора доменных имен Namecheap передать несколько доменных имен, которые имитировали Facebook и Instagram. бренды.

Среди перечисленных доменных имен были такие, как facbook-login.com, facbook-login.net, instagrarn.ai, instagrarn.net и instagrarn.org.

PROOFPOINT УТВЕРЖДАЕТ, ЧТО ПОХОЖИЕ ДОМЕНЫ - ЭТО ЧЕСТНАЯ ИГРА

В судебных документах, поданных во вторник, Proofpoint сказал, что UDRP не должна применяться к этим доменам, которые следует разрешить сохранить и продолжить использование.

Proofpoint утверждает, что запросы UDRP следует использовать только для доменов, зарегистрированных недобросовестно. Фирма по безопасности вместо этого заявляет, что она использовала похожие домены Facebook и Instagram «добросовестно и в законных целях».

Proofpoint утверждает, что ее тесты на осведомленность о фишинге имеют решающее значение для безопасности ее клиентов, но также и для безопасности самого Facebook, поскольку тесты на осведомленность о фишинге учат пользователей распознавать похожие домены Facebook и Instagram и фишинговые атаки - от чего Facebook также выигрывает, хотя косвенно.

Фирма безопасности также утверждает, что, хотя другие похожие домены используются для преступной деятельности, похожие домены Facebook, которыми она владеет, не являются оружием и не причиняют вреда пользователям.

По данным службы безопасности, пользователи, которые переходят по ссылкам, найденным в фишинговых тестах Proofpoint, всегда получают уведомление о том, что они выполнили нежелательное действие, учетные данные учетной записи Facebook не собираются или что пользователю причинен вред.

Кроме того, пользователи, которые получают доступ к доменам напрямую, также предупреждаются, что это не официальные сайты Facebook.

«Путаница среди потребителей маловероятна, потому что Proofpoint четко указывает на веб-сайтах, на которые указывают доменные имена: «Привет! Этот веб-сайт принадлежит программе Proofpoint Security Awareness Training. Этот домен используется для обучения сотрудников тому, как распознавать фишинговые атаки и избегать их».

Теперь Proofpoint хочет, чтобы судья вынес решение, разрешающее использование этих доменных имен «в связи с добросовестным предложением товаров или услуг» и добросовестно; следовательно, они не должны подвергаться классическому запросу UDRP об изъятии…». ***(Catalin Cimpanu. Proofpoint sues Facebook to get permission to use lookalike domains for phishing tests // ZDNet (https://www.zdnet.com/article/proofpoint-sues-facebook-to-get-permission-to-use-lookalike-domains-for-phishing-tests/). 11.02.2021).***

***

«Технологический сектор Индо-Тихоокеанского региона «созрел для инвестиций», по словам Триши Рэй, научного сотрудника исследовательского фонда Observer Research Foundation в области технологий и СМИ.

«Редкие земли, которые используются во всех наших устройствах, компьютерах, электромобилях и так далее, альтернативы ненадежным поставщикам 5G, даже инвестиции в базовую инфраструктуру для фибреизации сетей - все это созрело для инвестиций», - сказал Рэй во вторник.

«Большая часть региона, особенно Юго-Восточная Азия [и] Индия, являются основными сборочными узлами в мировой торговле технологиями, но необходимо уделять больше внимания основным компетенциям и наращиванию потенциала».

Один из примеров - полупроводники. В этом регионе находится множество заводов по производству чипов, но они, как правило, не разрабатывают чипы.

«Большая часть ценности полупроводников заключается в их дизайне, поэтому на долю Intel приходится четверть мировой стоимости полупроводников», - сказала она.

Рэй выступал на открытии сети Quad Tech Network (QTN), инициативы правительства Австралии по «продвижению регионального исследования второго уровня и общественного диалога по кибернетическим и критическим технологическим вопросам» между четырьмя участниками Четырехстороннего диалога по безопасности или «Quad ": Австралия, Индия, Япония и США.

QTN управляется Колледжем национальной безопасности Австралийского национального университета в Канберре.

Комментарии Рэя основывались на статье под названием «Цифровой Индо-Тихоокеанский регион: региональная взаимосвязь и устойчивость», с соавтором которой она выступила, - одной из четырех статей, выпущенных при запуске.

Его рекомендации включали разработку общих стандартов для цифровых услуг, таких как гармонизация национальных, а затем и региональных стандартов цифровых платежей; интероперабельные трансграничные цифровые идентификаторы; и улучшение цифровых навыков на всех уровнях.

В отчете отмечается, что результаты исследований Малайзии, Индии и Австралии «остаются намного ниже их потенциала». В то время как в Малайзии «высокий уровень квалифицированных специалистов в области цифровых технологий», а в Индонезии и Камбодже «не хватает базовых цифровых навыков».

И хотя Вьетнаму «необходимо лучше направлять свои технические таланты», Австралии «не хватает передовых цифровых навыков».

«Мы также уделяем большое внимание вопросам подключения в первую очередь, включая просто электричество, доступ к надежному высокоскоростному Интернету, цифровую грамотность, все это важные элементы», - сказал Рэй.

Согласно Martijn Rasser, соавтор Центра новой американской безопасности бумаги под названием Сети: Techno-дем для управления государством Австралии и Quad, то QTN является логическим расширением сферы компетенции Quad в.

«У вас есть значительная часть мирового ВВП и населения, общие интересы и ценности, а также общее понимание того, что потребуется для достижения экономической конкурентоспособности в ближайшие десятилетия, - сказал Рассер.

«В ближайшем будущем есть хорошая возможность добиться важных успехов в таких областях, как установление норм, способствующих свободному и открытому киберпространству, устранение уязвимостей цепочек поставок, таких как редкоземельные элементы, и стимулирование технологических инноваций для беспроводной инфраструктуры 5G».

Кибердипломатия Австралии уже сыграла ключевую роль в установлении международных норм кибербезопасности, хотя ее влияние снизилось при правительстве Моррисона.

ГДЕ 40-ЛЕТНЕЕ ТЕХНИЧЕСКОЕ ВИДЕНИЕ АВСТРАЛИИ?

Рассер рекомендовал каждой из четырех наций «разработать настоящую национальную стратегию в области технологий».

«Это требует видения. Где вы хотите быть через 20, 30, 40 лет?», - сказал он.

«В каких технологических областях вы хотите, чтобы ваша страна была мировым лидером? Где вы должны быть конкурентоспособными на мировом рынке? И где есть области, в которых вы можете позволить себе быстро следовать? Потому что вы не собираетесь быть номером один во всем, это просто недоступно, это недостижимо в конечном итоге».

Еще раз стоит отметить, что Стратегия кибербезопасности Австралии на 2020 год была разочаровывающе скучной и ориентированной на внутренний рынок, с небольшим расширением развития кибербезопасности за пределами стратегии 2016 года.

Здесь явно есть возможности для улучшения, и вашему корреспонденту ясно, что правительству Австралии необходимо будет активизировать свое технологическое мышление, чтобы решить эту проблему.

«Конечная цель этой стратегии должна заключаться в том, чтобы страна расширяла возможности своих граждан, экономически конкурировала и защищала свои национальные интересы, не подвергая опасности свои ценности или суверенитет», - сказал Рассер.

По словам профессора Джолиона Форда из юридического колледжа ANU, системы доверия, инклюзивности и управления являются дополнительными проблемами.

«Как вы берете с собой свои общества и вовлекаете их в разговоры о возможностях и проблемах управления и как включаете их в этот процесс?», - спросил Форд.

«[Как вы] укрепляете доверие не только к технологиям, но и к структурам, управляющим этими технологиями?»

По его словам, существуют ограничения для государственных и не государственных стратегий, особенно в таких областях, как искусственный интеллект (ИИ).

НЕПРОПОРЦИОНАЛЬНАЯ РОЛЬ КРУПНЫХ ТЕХНОЛОГИЙ

«Частный сектор и, в частности, крупные технологические компании играют такую непомерную или непропорциональную роль в формировании всего повествования об этих технологиях и их пользе или других вещах, а также в формировании возможностей моделей управления на основе этих технологий», - сказал Форд.

Форд является соавтором статьи «Охват различий: управление важнейшими технологиями в Индо-Тихоокеанском регионе», в которой рассматривались вопросы прав человека и этики.

Извечный вопрос о важности обмена разведданными о киберугрозах был поднят доктором Кохей Такахаши, исследователем из Национального института аспирантуры Японии по политическим исследованиям.

«Австралия и Соединенные Штаты уже работают над разведкой киберугроз в рамках Five Eyes. Поэтому для стран четверки важно создать новую структуру для эффективного обмена информацией о киберугрозах», - сказал он.

Такахаши также подчеркнул важность создания системы проверки фактов.

«Например, влияние операций в киберпространстве с помощью фейковых новостей стало большой проблемой. Для стран четверки важно создать систему проверки фактов», - сказал он.

В статье, в соавторстве с Такахаши, Cyber Security, Critical Technology, and National Security, также рекомендуются совместные исследования в области ИИ и совместные кибер-упражнения.

«В будущем ИИ будет использоваться в киберпространстве. Нам необходимо будет продвигать исследования и исследования в этой области, чтобы улучшить наши возможности взаимодействия», - сказал он.

«У каждой страны есть свои сильные и слабые стороны. Важно проводить совместные учения, чтобы использовать сильные стороны других потенциальных союзников и партнеров и повысить их устойчивость». ***(Stilgherrian. Indo-Pacific tech sector 'ripe for investment' and cyber defence cooperation: Research // ZDNet (https://www.zdnet.com/article/indo-pacific-tech-sector-ripe-for-investment-and-cyber-defence-cooperation-research/). 10.02.2021).***

***

«Сегодня, выступая в Деловом совете по международному взаимопониманию (BCIU), Брэндон Уэльс, исполняющий обязанности директора Агентства по кибербезопасности и безопасности инфраструктуры (CISA), объявил о выпуске первой в истории международной стратегии агентства, CISA Global. Во время беседы у камина с президентом и генеральным директором BCIU Питером Тихански и.о. директора Уэльс рассказал, как CISA будет работать с международными партнерами для выполнения миссии агентства и создания единства усилий во всех областях миссии.

«Сегодняшний глобально взаимосвязанный мир представляет широкий спектр серьезных рисков и угроз для критически важной инфраструктуры», - сказал исполняющий обязанности директора CISA Брэндон Уэльс. «Киберрискам, с которыми мы сталкиваемся, нет границ, и сейчас - более чем когда-либо - мы должны работать вместе. CISA Global описывает, как мы будем взаимодействовать с международными партнерами для наращивания потенциала CISA и усиления нашей способности защищаться от киберинцидентов, повышения безопасности и отказоустойчивости критически важной инфраструктуры, выявления и устранения наиболее значительных рисков для важнейших функций, а также обеспечения бесперебойной и безопасной работы в чрезвычайных ситуациях. коммуникации».

CISA Global описывает, как CISA будет использовать свою глобальную сеть для усиления партнерского потенциала и создания более совершенной коллективной практики и реагирования на неотложные угрозы, которые имеют решающее значение для интересов национальной безопасности США. Стратегия описывает международное видение CISA и определяет четыре цели:

Развитие оперативного сотрудничества;

Наращивание партнерского потенциала;

Укрепление сотрудничества посредством вовлечения заинтересованных сторон и разъяснительной работы; и

Формирование глобальной политической экосистемы.

CISA стремится к созданию открытого, функционально совместимого, надежного и безопасного взаимосвязанного мира в глобальной, операционной и политической среде, в которой защитники сети и менеджеры по рискам могут коллективно предотвращать и смягчать угрозы для критически важной инфраструктуры». ***(CISA RELEASES NEW GLOBAL STRATEGY FOR INTERNATIONAL ENGAGEMENT // Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/news/2021/02/18/cisa-releases-new-global-strategy-international-engagement). 18.02.2021).***

***

«Агентство по кибербезопасности и безопасности инфраструктуры (CISA) и CYBER.ORG совместно анонсируют серию видеороликов о кибербезопасности, чтобы помочь тем, кто учится или работает в Интернете, предпринять активные шаги для защиты себя и своего бизнеса. CYBER.ORG - это организация по развитию кадровых ресурсов в области кибербезопасности, которая нацелена на учащихся старших классов до 12 лет с осведомленностью о карьере в киберпространстве, учебными ресурсами и повышением квалификации учителей.

Тем не менее, серия видеороликов о кибербезопасности направлена на освещение соответствующих тем о кибербезопасности в серии коротких видеороликов, подходящих для всех граждан, а не только для учебных заведений K-12.

«По мере того, как страна - от работодателей до сотрудников и от учителей до студентов - сталкивается с новыми методами удаленной работы и дистанционного обучения, для всех нас становится все более важно знать некоторые передовые методы обеспечения безопасности в Интернете», - сказал Мэтт Хартман., Исполняющий обязанности помощника исполнительного директора по кибербезопасности, CISA. «С помощью коллективных и совместных подходов мы можем усложнить злоумышленникам киберпреступность воздействия на школы и бизнес. Наше партнерство с CYBER.ORG важно и помогает повысить осведомленность об основных, но надежных принципах поведения и действиях в области кибербезопасности и повысить их эффективность».

«Мы гордимся тем, что сотрудничаем с CISA, чтобы информировать общественность о том, как оставаться в безопасности в киберпространстве в то время, когда это больше всего необходимо», - сказал директор CYBER.ORG Кевин Нолтен. «С переходом на удаленную работу и онлайн-обучение кибер-злоумышленники разработали все более изощренные методы, зависящие от ошибок в протоколах безопасности по инициативе пользователей. Эти образовательные усилия имеют первостепенное значение для борьбы с внешними угрозами и обеспечения того, чтобы у общественности были образовательные инструменты для распознавания предупреждающих знаков».

В настоящее время серия видеороликов включает пять видеороликов, в которых представлены простые для понимания концепции кибербезопасности, и в ближайшие месяцы будет выпущено еще несколько видеороликов. В сочетании с кампанией по повышению осведомленности о программах-вымогателях CISA в

новейшем дополнении к этой серии содержатся советы, как не стать жертвой атаки программ-вымогателей.

Каждое видео длится менее трех минут и представлено в анимированном формате, который предлагает наблюдателям сравнить свои собственные практики с практиками персонажей на видео. В видеороликах зрителей побуждают придерживаться безопасных и надежных методов поведения, которые могут наилучшим образом защитить их конфиденциальность. К каждому видео прилагается информационный бюллетень с основными моментами и разговорами, которые можно использовать или распространять на собраниях или занятиях». ***(CISA AND CYBER.ORG PARTNER TO DELIVER CYBER SAFETY VIDEO SERIES // Cybersecurity and Infrastructure Security Agency (CISA) (https://www.cisa.gov/news/2021/02/09/cisa-and-cyberorg-partner-deliver-cyber-safety-video-series). 09.02.2021).***

***

«Кибербезопасность - это гонка вооружений, в которой преступники и компании постоянно сражаются за то, чтобы оставаться на шаг впереди друг друга. Пандемия просто предоставила хакерам большое преимущество.

Исследование, проведенное Opinium в партнерстве с Bird & Bird, показало, что в Лондоне три из пяти компаний (60%) утверждают, что удаленная работа увеличивает риск для их ИТ-инфраструктуры. Чуть менее половины (46%) заявили, что с марта 2020 года количество кибератак увеличилось. И более половины (55%) сообщают о значительном увеличении числа клиентов, заявивших, что они стали жертвами онлайн- или удаленных мошенников после пандемии началось.

По словам Саймона Шутера, партнера Bird & Bird в Лондоне и главы международной коммерческой группы, наблюдается всплеск активности со стороны всех типов кибератак.

«Внизу есть младший элемент, сценаристы. Сидят дома скучно, поэтому разминают мышцы. Немного поднявшись по пищевой цепочке, у вас есть хактивисты. Опять же, они дома со временем, поэтому их активность неизбежно возрастает.

«Еще есть киберпреступники. Они видят более целевую среду, потому что люди работают из дома и используют системы, которые могут быть значительно более уязвимыми, чем в их офисах. Таким образом, мы наблюдаем значительный отскок в атаках типа «злоумышленник в середине», когда злоумышленник перехватывает сообщения между двумя людьми и изменяет их, чтобы контролировать диалог.”

По словам Шутера, еще одна быстрорастущая область - это программы-вымогатели, которые становятся все более изощренными по мере того, как преступники начинают специализироваться в определенных секторах.

«Затем наверху у вас есть национальные государства и наемные хакеры. Они могут искать подробную информацию о вакцинах против COVID-19 или участвовать в политической деятельности. Происходит много шпионажа, и это область, о которой меньше всего известно, потому что, если они и хороши, они появляются и исчезают без следа.”

Причины бояться

Не только удаленная работа облегчила жизнь хакерам. В мае 2020 года McKinsey сообщила, что «мы продвинулись на пять лет вперед в внедрении цифровых технологий для потребителей и бизнеса всего за восемь недель. Это ускорение создало новые слабые места и сделало старые более заметными.

Клаудио Татаранни - директор консультационного подразделения Bird & Bird OXYGY. Он отмечает, что цифровая трансформация бизнеса автоматически делает его более уязвимым для кибератак, поскольку объединяет все данные компании и увеличивает ее зависимость от цифровых систем.

«Компании все чаще работают в сетях, поэтому безопасность цепочки поставок становится все более важной, - говорит он. «Кибератака может быть нацелена на крупную корпорацию, но хакерам может быть проще атаковать поставщиков этой корпорации, а затем перейти через сеть к корпорации.

«Интернет вещей также тесно связан с кибербезопасностью. Сейчас существует множество устройств, которые обмениваются данными внутри компаний, но также и между компаниями. Все они могут стать целями кибератаки.”

Любая новая технология создаст новые проблемы. Татаранни приводит пример искусственного интеллекта, возможно, самой большой новой технологии из всех.

«ИИ можно использовать, чтобы защитить нас; мы можем использовать алгоритмы, чтобы остановить атаку. Но он также может использоваться злоумышленниками для более изощренных атак, поскольку они могут адаптироваться к ответам компании.”

Вы так же небезопасны, как и ваша самая протекающая точка

Вся эта активность замедляться не собирается. Опрос также показал, что почти девять из десяти (88%) предприятий, которые столкнулись с повышенным риском для своей ИТ-инфраструктуры после перехода на удаленную работу, ожидают, что этот риск сохранится в течение следующих 12–18 месяцев.

Хорошая новость заключается в том, что ИТ-отделы становятся все лучше и лучше в повышении безопасности удаленных сетей. Плохая новость в том, что большинство взломов начинается не с технологий. Они начинаются с человеческого фактора, и удаленная работа выявила столько же человеческих уязвимостей, сколько и проблем с сетевой безопасностью.

«Все получают больше приглашений на видеоконференции в своих почтовых ящиках, а также произошел взрывной рост платформ электронной подписи, поэтому у вас есть угроза того, что сотрудники непреднамеренно нажмут на любые средства связи», - объясняет Дэйв Кинг, генеральный директор Digitalis. специализированная компания по управлению цифровыми рисками и репутацией в Интернете. «Хакеры воспользуются этим, поэтому мы наблюдаем рост количества как общих фишинговых атак со ссылками на вредоносное ПО, так и сложных индивидуальных атак.»

Поэтому советуем не спрашивать, подвергнется ли ваша компания нападению, а когда. Проблема в том, что большинство компаний по-прежнему считают кибербезопасность проблемой ИТ.

«Когда я говорю с клиентами о кибербезопасности, единственные люди, с которыми я встречаюсь, - это ИТ-команда, - говорит Шутер. «Я редко встречаю даже охрану старого образца. Но компаниям нужен целостный подход к безопасности; Вы в безопасности настолько, насколько сможете.”

Эта точка может быть где угодно. Это может быть фишинговое письмо, на которое кто-то нажимает, не задумываясь; это может быть USB-накопитель, оставленный в машине на парковке компании. Как отмечает Шутер, удаленная работа означает, что в большинстве лондонских офисов сейчас работает скелетный персонал, который может не знать текущих процедур безопасности и может не знать, кто должен приходить и уходить. Все это создает точки уязвимости.

Доллар останавливается на генеральном директоре

Итак, первое, что нужно задать совету директоров компании, - это какие изменения были внесены в меры безопасности с начала пандемии.

«Совет директоров должен запросить анализ того, подвержена ли компания большему риску, и что было сделано для решения этой проблемы; программа для подключения удаленной рабочей силы; и грамотный анализ киберстрахования компании, - говорит Шутер. «Им также следует спросить о том, что было сделано для информирования персонала компании о рисках.”

Однако, в конечном итоге, изменение в понимании и устранении уязвимостей человека должно происходить под руководством генерального директора.

«Мы говорим генеральному директору: продолжайте инвестировать в оборудование и программное обеспечение, продолжайте поддерживать своего технического директора и своего ИТ-директора», - говорит Кинг. «Но если вы не инвестируете в снижение уязвимости человека, вы можете полностью урезать их бюджет, потому что в этом нет смысла.»

Снижение уязвимости человека

Инвестиции в эту человеческую сторону кибербезопасности должны охватывать ряд областей. Персонал должен пройти обучение по вопросам безопасности, чтобы убедиться, что они понимают, что безопасность - это ответственность каждого. Как указывает Дэвид Уайт, основатель платформы управления, рисков и соответствия Esorma, одним из признаков того, что сообщение доходит, является то, что вы начнете получать больше предупреждений безопасности.

Еще одно, что нужно сделать прямо сейчас, - говорит Уайт, - это подумать о том, у кого к каким данным есть доступ.

«У большинства компаний есть системы контроля доступа, так что это бесплатное решение», - объясняет он. «Важно ограничить доступ к конфиденциальным данным - странные вещи могут происходить, когда неподходящие люди получают доступ к данным. Точно так же важно не чрезмерно ограничивать доступ, потому что это приводит к тому, что люди находят обходные пути, которые в основном являются кибер-нарушениями с благими намерениями и могут быть использованы, если персонал лишится гражданских прав.”

По словам Кинга, что-то еще, что следует сделать немедленно, - это изучить то, что называется «поверхностью атаки» компании; сумма потенциальных точек входа для злоумышленника.

«Злоумышленник будет смотреть на генерального директора, на его секретаря, его жену и своих детей, чтобы увидеть, что там, скрыто в глубокой сети, что они могут собрать воедино и использовать в атаке», - объясняет Кинг. «Если вы все это знаете, вы можете поговорить с людьми о смягчении последствий. Вы можете сделать эти социальные платформы приватными, вы можете удалить вещи, которые выдают слишком много информации. Теперь это должно быть стандартной рабочей процедурой для совета директоров, чтобы провести аудит атак, чтобы понять, что там происходит."

«Это также имеет второстепенные преимущества. Он указывает на то, что может нанести репутационный ущерб. И это может помочь в обеспечении физической безопасности, потому что эти же методы все чаще используются преступниками в физическом мире для организации краж со взломом или, на других территориях, похищений."

План выздоровления

Уайт рекомендует другой способ преодоления разрыва между технологическими и человеческими аспектами кибербезопасности, который можно быстро реализовать - план обеспечения непрерывности бизнеса и аварийного восстановления.

«Люди работают разрозненно, - говорит он. «ИТ-команда обычно не общается за пределами своего отдела. Но если вы начнете создавать план обеспечения непрерывности бизнеса, вы больше не будете говорить об ИТ. Вы автоматически общаетесь с остальной частью бизнеса и вносите безопасность в их бункер.

«В процессе обеспечения непрерывности бизнеса вы определяете абсолютные ключевые активы бизнеса, о которых необходимо заботиться, что бы ни случилось, и вы решаете, как их защитить. Но бизнес всегда меняется, потому что меняются потребности клиентов. Так нужно ли защищать то, что требовало защиты? Или надо сегодня по-разному защитить? Вам нужно каждые шесть месяцев репетировать, что идет не так, чтобы увидеть, работает ли ваш план."

Все это может показаться очевидным, но исследование 2019 года, проведенное поставщиком технологических услуг Probrand, показало, что четверть британских малых и средних предприятий не имеют плана обеспечения непрерывности бизнеса, а половина из них не тестирует его регулярно.

Shooter приводит в пример недавнюю работу с небольшим инвестиционным банком над его программой киберустойчивости. Это включало обзор и пересмотр планов реагирования; подготовка руководств по таким вопросам, как соблюдение требований финансового законодательства, управление персоналом и конфиденциальность данных в контексте инцидента; создание круглосуточной дежурной службы экстренной помощи; и проведение обучения и участие в симуляционных упражнениях.

«Все это приводит к тому, что клиент может продемонстрировать соответствие требованиям регулирующего органа», - говорит он. «Не менее важно то, что это означает, что клиент не только лучше защищен от атаки, но и способен справиться с инцидентом в случае его возникновения."

Законодательство и регулирование

Еще одна вещь, о которой должно знать руководство компании, - это то, как меняются законодательство и нормативные акты, касающиеся кибербезопасности. Несмотря на то, что Brexit теперь «готов», законы и директивы ЕС по-прежнему применяются к компаниям из стран, не входящих в ЕС (теперь включая Великобританию), которые предоставляют свои услуги в ЕС. Bird & Bird's Shooter предупреждает, что директива Директивы по сетевым и информационным службам (NIS) должна серьезно измениться в рамках стратегии кибербезопасности ЕС на Цифровое десятилетие. Предложение о директиве о мерах по обеспечению высокого общего уровня кибербезопасности в ЕС, известное как NIS 2, было представлено в декабре 2020 года, а период обратной связи должен завершиться 18 марта этого года.

«Мы должны знать, что правила ЕС и Великобритании по передаче данных должны вступать в брак, иначе мы очень усложняем себе жизнь», - говорит Шутер. «Великобритания в настоящее время полностью синхронизирована с Европой, поэтому будет интересно посмотреть, пойдем ли мы в ногу со временем и внесем поправки в правила NIS. ”

Кроме того, 27 июня 2020 года вступил в силу Закон ЕС о кибербезопасности, укрепивший агентство ЕС по кибербезопасности Enisa и установив общеевропейскую систему сертификации кибербезопасности для продуктов, процессов и услуг ИКТ. Великобритания рассматривает собственное законодательство или свод правил для смарт-устройств, и, по словам Шутера, мы можем ожидать, что это будет копировать то, что существует в ЕС. Он предупреждает, что производители и поставщики соответствующих устройств должны быть в курсе разработок EUCA, так как они могут повлиять на возможность продажи их продуктов.

«Команды комплаенс должны следить за всем этим и стремиться обеспечить соблюдение требований как можно раньше. Это всегда сложнее и дороже, когда к голове приставлен пистолет», - говорит он.

«Более широкое и целенаправленное регулирование предполагает выполнение обязательств, и это прерогатива юриста. Разработка, внедрение, мониторинг и корректировка программ комплаенс - это основная задача таких юристов, как мы. Вам следует привлечь внешнюю юридическую экспертизу, как только начнется отсчет времени с соблюдением нормативных требований.”

После приступа

Компании могут многое сделать, чтобы избежать кибератак и смягчить их последствия, но рано или поздно они пострадают. По словам Шутера, если это атака программы-вымогателя, многие компании считают, что заплатить дешевле и проще, чем пытаться перезапустить бизнес.

«Запрещается платить выкуп только в том случае, если деньги идут запрещенной организации, например, террористической группе, но вы редко узнаете, так ли это», - говорит он. «Это также часто покрывается страховкой, но компании должны проверить свою политику. Он не будет покрываться, если платеж незаконен.”

Шутер объясняет, что после оплаты компании обычно возвращают свои данные или ключ, необходимый для их разблокировки. «После этого вы, как

правило, больше не будете поражены тем же нападающим», - говорит он. Но он предупреждает, что где-то в даркнете вы будете идентифицированы другими преступниками как заплатившие. Обычно это означает найм эксперта по кибербезопасности, который проверит вашу безопасность и устранит любые лазейки.

По словам Шутера, устранение последствий атаки - еще одна область, в которой компаниям следует обращаться за помощью к специалистам.

«Это все более юридический вопрос. Есть возможность регулирующего расследования; групповые действия от имени пострадавших от атаки владельцев данных; судебный процесс на основе последствий, например, если кто-то доверил вам конфиденциальные данные, которые были украдены в результате атаки, они могут подать в суд. Работа со всем этим носит технический характер, может быть сложной и часто требует опыта, которого нет в компании.”

Это процесс, а не проект

Реакция предприятий на пандемию COVID-19 дала кибератакам множество новых уязвимостей, которые можно использовать, и гораздо больше времени для их использования. Из-за того, что блокировки, вероятно, будут продолжаться в различных формах в течение нескольких месяцев, а люди, вероятно, предпочтут работать из дома гораздо дольше после этого, компаниям необходимо изменить свое отношение к кибербезопасности.

«ИТ-менеджер или даже член совета директоров могут рассматривать безопасность как проект, у которого есть начало и конец, но на самом деле безопасность - это программа, - предупреждает Уайт.

Стрелок соглашается.

«Это бесконечная гонка вооружений между хакером и защитником», - говорит он. «Как защитники вы обычно немного отстаете, но если вы можете держать ситуацию под контролем, это можно сделать терпимым.» ***(Simon Shooter. London & the hacker // Bird & Bird (https://www.twobirds.com/en/news/articles/2021/uk/london-and-the-hacker). 10.02.2021).***

***

«Мировой индекс киберрисков, по мнению аналитиков Ponemon Institute, остается достаточно негативным. Это связано и с удручающей статистикой 2020 г., и с тревожными ожиданиями от 2021 г.

В мире констатирован повышенный риск киберугроз

Почти четверть всех компаний мира в 2020 г. семь или более раз подвергались атакам кибепреступников. Такие данные содержатся в отчете экспертов Ponemon Institute, которые составили ежегодный индекс киберрисков Trend Micro. По мнению участников исследования, в 2021 г. ситуация будет только ухудшаться. Подавляющее большинство опрошенных (83%) ожидают, что такие кибератаки с «некоторой» или «очень высокой» вероятностью окажутся успешными.

Прямо сейчас глобальный индекс киберрисков составляет -0,41 балла по шкале от -10 (наихудшая ситуация) до 10 (наилучшая ситуация). Такой уровень

соответствует повышенному риску, хотя в отдельных странах он еще негативнее. Например, в США он составляет -1,07, что аналитики связывают с плохой готовностью американских компаний к отражению киберугроз в сравнении с организациями из других регионов мира. Для сравнения, в регионе EMEA отмечен уровень -0,13, а в регионе APAC — -0,02.

Больше всего компании боятся потери данных клиентов

Основными способами атак по итогам 2020 г. компании назвали фишинг и социальную инженерию, использование программ-вымогателей и ботнетов, бесфайловые атаки и атаки типа «человек посередине». В число наиболее пугающих последствий активных действий киберпреступников организации включили потерю данных клиентов и их последующий отток, утрату доступа к интеллектуальной собственности и финансовой информации, а также повреждение оборудования.

Здесь на страновом уровне тоже есть определенные отличия. Например, только в американских организациях в число негативных последствий атак включили расходы на внешних ИБ-специалистов и консультантов. А в регионе APAC упомянули о потенциальном ущербе критически важной инфраструктуре.

Если говорить именно об инфраструктурных угрозах, то тут респонденты выделили организационную несогласованность, небрежность инсайдеров, потенциальные проблемы с облаками, нехватку квалифицированных кадров.

«В 2020 году мы увидели, насколько драматическими могут быть масштабы использования киберпреступниками пандемии для проведения целевых кибератак по всему миру. Согласно отчету FortiGuard Labs о ландшафте угроз, в первой половине 2020 года организации в США, Китае и России были наиболее частыми объектами атак, так или иначе связанных с темой коронавируса, — говорит Михаил Родионов, региональный директор Fortinet в России и странах СНГ. — Пандемия лишь усилила то, о чем многие профессионалы отрасли говорили в течение довольно продолжительного времени: чтобы построить действительно эффективную защиту от киберугроз, нужна постоянная бдительность и способность адаптироваться к меняющимся стратегиям преступников. Лучший способ защиты от постоянно растущей активности вредоносов — комплексный, интегрированный подход к ИБ. Его важным компонентом является постоянный доступ к новейшей информации об угрозах и обучение по кибербезопасности». ***(Каждую четвертую компанию мира в 2020 г. атаковали больше 7 раз // CNews (https://safe.cnews.ru/news/top/2021-02-04_kazhduyu_chetvertuyu_kompaniyu). 08.02.2021).***

***

«На фоне сбоев, связанных с пандемией Covid-19 и кампанией кибершпионажа SolarWinds, NYDFS выпустила руководство для страховщиков, которые подписывают полисы киберстрахования, и которое содержит ряд положений, которые, как ожидается, повлияют на компании, подающие заявки на страхование от киберпространства или возобновляющие его. Не в последнюю очередь это конкретная рекомендация, согласно которой страховщики требуют от страхователей сообщать о происшествиях в области

кибербезопасности в правоохранительные органы. Хотя технически это не является частью семиуровневой системы рисков киберстрахования, руководство NYDFS включает в себя конкретную рекомендацию против совершения выкупа в ответ на инциденты, связанные с кибербезопасностью вымогателей.

В руководстве изложена система рисков киберстрахования (далее «Структура»), которая предоставляет передовые методы управления рисками киберстрахования на фоне опасений NYDFS, что страховщики не могут точно измерить киберриски, что может представлять как системные, так и «скрытые» риски для финансовый сектор. Руководство предлагает обширное влияние компрометации SolarWinds в качестве примера системного риска, а компрометация SolarWinds и инцидент NotPetya 2017 года - в качестве примера скрытого риска, при котором страховщики несут убытки от киберинцидентов, покрытие киберинцидентов неясно или нет. явным образом в условиях политики. NYDFS по-прежнему обеспокоена тем, что этот скрытый риск остается значительной проблемой для многих страховых компаний.

Концепция разъясняет ожидания NYDFS, что страховщики, которые подписывают полисы киберстрахования, разработают «строгий и основанный на данных подход» к управлению киберрисками и что решения страховщиков относительно предложения и цены киберстрахования для конкретных организаций «должны основываться на тщательная оценка риска этой организации». NYDFS признала, что риск страховщиков зависит от размера, ресурсов, географии, доли рынка и страховых компаний, поэтому каждый страховщик должен придерживаться соответствующего индивидуального подхода, основанного на оценке риска, при принятии следующих передовых практик:

Разработать официальную стратегию рисков киберстрахования - эта стратегия должна направляться высшим руководством и утверждаться на самом высоком уровне компании (например, Советом директоров), и включать «четкие качественные и количественные цели риска», которые отслеживаются по результатам деятельности и сообщаются. высшему руководству и Совету директоров на регулярной основе. Эта стратегия должна включать оставшиеся шесть передовых практик из Рамочной основы.

Управление и устранение подверженности риску скрытого киберстрахования - Оцените и уменьшите подверженность скрытому риску в краткосрочной перспективе и устраните скрытый риск в долгосрочной перспективе путем пересмотра условий полисов в будущем и приобретения перестрахования в промежуточном периоде.

Оценка системного риска - Проведите внутреннее стресс-тестирование на основе маловероятных катастрофических кибер-событий, которые учитывают как скрытый, так и утвердительный риск, и включают сценарии стресс-тестирования, которые учитывают конкретные риски для предлагаемых продуктов и вариации в разных отраслях страховых компаний. Извлеченные уроки и выявленные потенциальные убытки должны быть включены в общую стратегию киберстрахования.

Тщательно оценивайте застрахованный риск - Страховщики должны подробно оценить программу кибербезопасности застрахованного, в том числе

посредством интервью, опросов и соответствующих сторонних или внешних оценок рисков, а затем сравнить эту информацию с историей страховых требований, чтобы выявить пробелы в мерах кибербезопасности, которые могут иметь место. об определении риска страховщиком. Мы отмечаем, что темы, перечисленные в качестве базовых для определения объема оценки, слабо соответствуют положениям Требований кибербезопасности NYDFS (23 NYCRR 500).

Обучайте страховщиков и производителей страховых услуг. Страховщики должны предоставлять исчерпывающую информацию и ресурсы, которые просвещают и стимулируют страхователей к принятию надежных программ кибербезопасности, а также сообщают страхователям об ограничениях полисов киберстрахования. NYDFS рекомендует страховщикам «стимулировать принятие более эффективных мер кибербезопасности с помощью политики ценообразования, основанной на эффективности программы кибербезопасности каждого застрахованного».

Получите опыт в области кибербезопасности. Страховщики должны нанимать, обучать и развивать свой персонал, чтобы понимать и оценивать киберриски, и при необходимости дополнять их консультантами.

Требовать уведомления правоохранительных органов - полисы киберстрахования должны требовать, чтобы нарушенные субъекты уведомляли правоохранительные органы с учетом общественных интересов, сдерживания преступности, потенциала правоохранительных органов для оказания помощи застрахованной жертве и повышения репутации застрахованного лица в плане надлежащего реагирования на инциденты. Примерно 36% респондентов опроса NYDFS уже требуют, чтобы их страховые компании уведомляли правоохранительные органы о киберинцидентах.

Хотя Стандарт применяется ко всем уполномоченным страховщикам имущества и от несчастных случаев, которые оформляют киберстрахование, в руководстве NYDFS говорится, что даже страховщики, которые не оформляют киберстрахование, должны оценивать свою подверженность «скрытому» риску и принимать соответствующие меры для снижения этого риска.

В NYDFS не указан график внедрения передовой практики, сформулированной в Концепции, но регулируемым организациям было бы разумно учитывать эти ожидания, особенно в контексте подготовки к экзаменам и недавнего активного взаимодействия NYDFS с регулируемыми организациями в ответ угрозам кибербезопасности, актуальным для финансового сектора.

Точно так же компании, которые могут подавать или продлевать полисы киберстрахования, могут пожелать рассмотреть свою относительную готовность к усилению осмотрительности на этапе андеррайтинга, включая тщательное изучение любых скрытых рисков, связанных с текущим покрытием, а также недавних улучшений безопасности и их отношения к прошлым претензиям. данные. Компании также могут пожелать внутренне проанализировать и оценить свой подход к оплате программ-вымогателей, включая меры безопасности и технические меры, реализованные для снижения риска успешных атак программ-вымогателей или связанных с ними сбоев в работе служб. Компании также могут

захотеть провести внутреннюю проверку и оценку своего подхода к сообщению об инцидентах правоохранительным органам». ***(Kate Hanniford. NYDFS Issues Best Practices for Cyber Insurance Risk Management // Alston & Bird (https://www.alstonprivacy.com/nydfs-issues-best-practices-for-cyber-insurance-risk-management/?cn-reloaded=1). 18.02.2021).***

***

«Хотя это и очевидно, Всемирный экономический форум в партнерстве с Marsh McLennan, SK Group и Zurich Insurance Group недавно выпустил свое 16-е издание Доклада о глобальных рисках (Отчет), в котором анализируются «риски социальных расколов, проявляющиеся в постоянных и новые риски для здоровья человека, рост безработицы, усиление цифрового разрыва, разочарование молодежи и геополитическая фрагментация» и определили, что кибератаки являются «ключевыми угрозами следующего десятилетия».

В отчете описываются серьезные риски, в том числе пандемия COVID-19, долговые кризисы, изменение климата и множество других прогнозируемых заболеваний, а кибербезопасность является одним из главных рисков. В отчете кибератаки упоминаются как риск с 2012 года, и, безусловно, сегодня этот риск гораздо более распространен, чем в прошлом.

Отказ кибербезопасности указан как «самый высокий риск по вероятности» в течение следующего десятилетия. Выход из строя ИТ-инфраструктуры является «одним из самых серьезных рисков следующего десятилетия». Просматривая карту ландшафта развивающихся рисков, кибератаки, мошенничество или кража данных переместились в верхнюю часть списка в качестве кластера.

При подготовке к глобальным рискам, изложенным в отчете, Всемирный экономический форум, хотя и назвал риски, описанные в отчете, «ужасными», предположил, что, размышляя о следующем кризисе после COVID-19, «[T] он ответ на COVID-19 предлагает четыре возможности управления для повышения общей устойчивости стран, предприятий и международного сообщества: (1) формулирование аналитических рамок, которые принимают целостный и системный взгляд на воздействия рисков; (2) инвестирование в известных «защитников рисков» для поощрения национального лидерства и международного сотрудничества; (3) улучшение информирования о рисках и борьба с дезинформацией; и (4) изучение новых форм государственно-частного партнерства по обеспечению готовности к рискам».

Хотя Отчет предельно честен и прозрачен в своих прогнозах, он, возможно, является моментальным снимком будущего, который бизнес-лидеры должны учитывать при планировании долгосрочных бизнес-стратегий, включая управление основными рисками по вероятности и влиянию на организацию. Это, очевидно, будет включать готовность к кибербезопасности и устойчивость». ***(Linn Foster Freedman. Cyber-attacks and Cybersecurity Failure Are Top Risks of the Next Decade Says World Economic Forum // Robinson & Cole LLP (https://www.dataprivacyandsecurityinsider.com/2021/02/cyberattacks-and-cybersecurity-failure-top-risks-of-the-next-decade-says-world-economic-***

forum/?utm_source=feedburner&utm_medium=feed&utm_campaign=feed%3a+dataprivacyandsecurityinsider+%28data+privacy+%2b+security+insider%29). 11.02.2021).

***

«Claroty сообщает, что злоумышленники, руководители по информационной безопасности и исследователи сосредоточили свое внимание на поиске критических ошибок безопасности в сетях АСУ ТП.

Он включен: согласно последнему отчету Claroty о рисках и уязвимостях ICS за два года, злоумышленники, директора по информационной безопасности и исследователи одновременно участвуют в безумной гонке за поиском уязвимостей кибербезопасности, скрывающихся в промышленных сетях.

В отчете были проанализированы все публично раскрытые уязвимости в сетях АСУ ТП во второй половине 2020 года, и было обнаружено, что количество раскрытий АСУ ТП увеличилось почти на 33% по сравнению с 2018 годом как со стороны таких организаций, как Claroty, так и от независимых исследователей.

Отрасли, в которых раскрывается больше всего, включают жизненно важные компоненты инфраструктуры, такие как критически важные производственные предприятия, энергетика, водоснабжение, сточные воды и коммерческие объекты.

Что еще хуже, более 71 процента ошибок можно было использовать удаленно, и каждое раскрытие во второй половине 2020 года занимало высокое место в списке 25 самых опасных уязвимостей программного обеспечения MITRE 2020 CWE за 2020 год, поскольку их легко использовать и они потенциально катастрофичны, говорится в отчете.

Кибербезопасность АСУ ТП привлекает исследователей

Во второй половине 2020 года Claroty насчитала 449 уязвимостей, обнаруженных у 59 поставщиков АСУ ТП; а за весь год их было 893. Для сравнения: в 2018 году общее количество обнаруженных ошибок АСУ ТП за весь год составило 672, а в 2019 году - 716, сообщает Claroty.

В докладе говорится, что все чаще эти отчеты поступают от независимых исследователей. Фактически, Claroty обнаружила, что во второй половине 2020 года 50 новых исследователей опубликовали раскрытия информации, которые не публиковались в течение двух предыдущих лет.

«Произошел сдвиг в сторону исследований АСУ ТП с сильным ростом групп исследователей безопасности для этого второго полугодового отчета, поскольку все больше организаций пытаются понять новый ландшафт атак», - пояснил Threatpost Амир Премингер, вице-президент по исследованиям в Claroty. «С увеличением количества игроков, которые выходят на рынок и уделяют особое внимание безопасности АСУ ТП, естественно, возрастет количество обнаруженных уязвимостей».

Злоумышленники обращают внимание на промышленные ошибки

Злоумышленники также усиливают давление на промышленные сети. Например, Claroty заметил добавление промышленных процессов в список уничтоженных программ- вымогателей Snake.

«Среда АСУ ТП стала более привлекательной целью для киберпреступников, и этот стимул связан не только с тем, что причинит наибольший ущерб, но и с тем,

какое оборудование они могут получить в свои руки», - сказал Премингер. «Атаки будут становиться все более изощренными и целенаправленными, поэтому важно, чтобы организации использовали разные стены обнаружения и тщательно практиковали безопасность».

Унаследованные системы с длительным сроком хранения также являются слабыми местами.

«В то время как исследования уязвимостей ICS и SCADA набирают обороты, многие проблемы безопасности, возникшие десятилетиями, еще не раскрыты», - поясняется в отчете. «В настоящее время злоумышленники могут иметь преимущество в их использовании, потому что защитники часто сталкиваются с ограничениями из-за требований к времени безотказной работы и растущей потребности в возможностях обнаружения уязвимостей, которые можно использовать, которые могут привести к прерыванию процесса или манипуляции».

Директора по информационной безопасности ICS и ПТСР SolarWinds

В отчете добавлено, что заголовки об атаке SolarWinds заставили руководителей по информационным технологиям в каждой отрасли дважды подумать о масштабах своих сетей и о том, кто может захотеть атаковать их.

«Национальные субъекты явно смотрят на многие аспекты периметра сети для использования, а киберпреступники также уделяют особое внимание процессам АСУ ТП, что подчеркивает необходимость таких технологий безопасности, как обнаружение на основе сети и безопасный удаленный доступ в промышленных средах», Премингер добавил.

Хорошая новость в том, что индустрия начинает реагировать.

«Отрадно видеть растущий интерес к АСУ ТП в сообществе исследователей безопасности, поскольку мы должны пролить более яркий свет на эти уязвимости, чтобы держать угрозы на расстоянии вытянутой руки», - сказал Премингер. «Выявление большего количества уязвимостей означает, что отрасль более защищена, поэтому обнадеживает то, что сообщество специалистов по безопасности относится к этому серьезно». ***(Becky Bracken. Industrial Networks See Sharp Uptick in Hackable Security Holes // Threatpost (https://threatpost.com/industrial-networks-hackable-security-holes/163708/). 05.02.2021).***

***

Сполучені Штати Америки

«Huawei снова подала иск против правительства США, на этот раз начав борьбу с Федеральной комиссией по связи (FCC) за ее решение обозначить компанию как угрозу национальной безопасности.

Согласно юридической жалобе, Huawei требует пересмотра назначения на том основании, что выполнение заказа выходит за рамки полномочий FCC; нарушил федеральный закон и Конституцию; произвол, своенравие и злоупотребление усмотрением; и не подтверждены существенными доказательствами.

Huawei также сообщила в жалобе, что назначение может отрицательно повлиять на финансовые интересы телекоммуникационной отрасли в целом.

FCC обозначила Huawei, наряду с ZTE, угрозой национальной безопасности еще в июне, в результате чего американские операторы связи больше не могут использовать Фонд универсальных услуг FCC для покупки оборудования или услуг у этих китайских компаний.

Уходящий председатель FCC Аджит Пай сказал, что в то время было «подавляющее количество доказательств» того, что и Huawei, и ZTE имели тесные связи с Коммунистической партией Китая и военным аппаратом Китая.

Обозначение возникло после того, как бывший президент США Дональд Трамп подписал закон, запрещающий компаниям США использовать федеральные средства для покупки оборудования у компаний, которые считаются угрозой национальной безопасности.

Закон также установил программу возмещения расходов в размере 1 миллиарда долларов, чтобы помочь более мелким провайдерам с расходами на демонтаж и замену запрещенного оборудования от Huawei и ZTE.

FCC - не единственное федеральное агентство, которое столкнулось с судебным иском со стороны Huawei. Вскоре после того, как Министерство торговли США добавило Huawei в свой «Список организаций», который запрещает американским компаниям передавать технологии Huawei без одобренной правительством лицензии, Huawei подала иск против агентства, утверждая, что оно действовало неконституционно при обеспечении соблюдения запрета.

В конце концов, этот иск был отклонен в феврале прошлого года на том основании, что Конгресс был в пределах своих прав обеспечивать соблюдение запрета.

«Заключение контрактов с федеральным правительством - это привилегия, а не право, гарантированное конституцией - по крайней мере, насколько известно этому суду», - заявил окружной судья Амос Маззант в своем февральском постановлении, рассматривая аргументы Huawei.

Huawei также подала иск с требованием об отмене закона, обеспечивающего соблюдение запрета. Этот иск все еще рассматривается в судах». ***(Campbell Kwan. Huawei requests US courts to overturn its national security threat designation // ZDNet (https://www.zdnet.com/article/huawei-requests-us-courts-to-overturn-its-national-security-threat-designation/). 10.02.2021).***

***

«После консультаций с отраслевыми экспертами Департамент финансовых услуг Нью-Йорка (DFS) изучил способы улучшения как рынка киберстрахования, так и кибербезопасности. В результате 4 февраля 2021 г. в Циркулярном письме № 2 по страхованию была опубликована система рисков киберстрахования.

Подход Концепции включает передовые практики для страховой отрасли при анализе рисков, но позволяет каждому страховщику рассчитывать свой собственный риск на основе гибких факторов, таких как размер страховщика, география, отрасли и ресурсы.

Раньше киберстрахование было необходимо только для сложных международных конгломератов. По оценкам, к 2025 году рынок киберстрахования в США превысит 20 миллиардов долларов.

Частично эта тенденция роста связана с распространением атак программ-вымогателей. По данным DFS, количество атак почти удвоилось в 2020 году, а средняя стоимость таких претензий выросла на 150%.

При таком резком увеличении затрат и атак очень важно, чтобы страховая отрасль принимала активное участие в борьбе.

Система киберстрахования рисков

Система рисков киберстрахования DFS состоит из семи этапов:

Разработать официальную стратегию киберстрахования рисков

Если страховщик предлагает киберстрахование, руководство страховщика должно разработать формальную стратегию оценки риска киберстрахования. Руководству следует определить соответствующий качественный и количественный максимальный риск и постоянно отслеживать, где падает текущий риск.

Стратегия должна включать шесть шагов ниже.

Управляйте и устраняйте риски скрытого киберстрахования

Наилучшая практика: укажите, будет ли кибер-убыток покрыт какой-либо политикой, в рамках которой возможно предъявление кибер-иска.

Скрытый кибер-риск возникает, когда страховщики в конечном итоге покрывают убытки, вызванные киберинцидентами, в соответствии с политиками, которые не были написаны для кибер-использования. Все политики - будь то имущество, несчастные случаи, общая ответственность, кража со взломом и т. Д. - должны быть оценены на предмет киберриска, чтобы ограничить размер непредвиденных убытков, причиненных кибернетикой в соответствии с этими политиками.

В конце концов, со временем это требование будет снято после преждевременного устранения скрытых рисков.

В случае действующих полисов страховщикам может быть выгодно приобрести перестрахование для покрытия скрытых киберрисков.

Оценить системный риск

Лучшая практика: постоянная оценка системного риска и планирование убытков.

Системный риск возникает из-за все более широкого использования сторонних поставщиков и поставщиков услуг. Очень важно, чтобы страховщики понимали зависимость страхователей от третьих сторон. Когда эти стороны скомпрометированы, это может нанести страховщикам значительные убытки, как в случае атаки трояна SolarWinds.

Проведение «внутренних стресс-тестов кибербезопасности на основе маловероятных, но реалистичных катастрофических киберсобытий» позволяет страховщикам анализировать свои потенциальные риски и убытки в различных отраслях. Эта информация может быть использована для создания более полной картины стратегии киберстрахования на этапе 1.

Тщательно оценивайте страховой риск

Страховщикам необходимо запрашивать подробную, основанную на данных информацию от каждого застрахованного в киберпространстве.

Такую информацию также следует запрашивать у третьих лиц, которые работают со страхователем.

Страховщики могут использовать собранную информацию для оценки слабых мест в существующем плане кибербезопасности страхователя.

Обучайте страховых компаний и страхователей

Передовой опыт: Страховщики должны активно участвовать в разработке киберполитик, начиная от типов и масштабов до допустимых пределов.

Регулярное информирование страховых компаний о новых рисках и подверженностях создаст более сильную политику.

Лучшая практика: предоставьте образование, скидки на планирование кибербезопасности и рекомендации для страхователей.

Страховщики и застрахованные получают выгоду, когда страхователи реализуют более строгие программы кибербезопасности. Страховщики должны повышать цены на киберполисы, если у конкретного страхователя слабая программа кибербезопасности, и снижать цены для тех, у кого есть продвинутые и эффективные киберполитики.

Получите опыт кибербезопасности

Важно, чтобы страховщики понимали меняющийся характер кибербезопасности. Это требует от страховщиков нанимать опытных киберпрофессионалов и регулярно обучать свой штат.

Требовать уведомления правоохранительных органов

Лучшая практика: уведомить правоохранительные органы о киберинциденте.

Следует разработать правила, требующие уведомления правоохранительных органов. Уведомление помогает страховщикам, страховщикам и общественности собирать информацию, восстанавливать то, что было украдено, и ловить виновных, ограничивая количество будущих атак.

Страховщикам следует помнить о трех вещах

Тихие риски

Системные риски

Образование и обучение

Страховщики должны быть особенно осведомлены о скрытых рисках. Независимо от типа политики, страховщики могут внезапно столкнуться с огромными убытками, вызванными киберинцидентами в рамках политики, не относящейся к киберпространству.

Системный риск - это еще одна проблема, когда один киберинцидент причиняет убытки многим страхователям. Учитывая продолжающийся кризис, вызванный компромиссом SolarWinds с Orion, страховщики должны знать об этом потенциале и заранее планировать такие разрушительные убытки.

Страховщикам и их страхователям будет в равной степени выгодно, если страховщики будут проводить расширенное обучение по вопросам кибербезопасности и соблюдение нормативных требований. Страхователи потенциально могут получить сниженный страховой тариф, если они пройдут обучение по киберстрахованию и соблюдают его. Страховщики будут вынуждены

оплачивать счета за меньшее количество предотвратимых киберинцидентов…» ***(Seven Points to Know in New Cyberinsurance Guidance that Help Companies and Insurers // Adams and Reese LLP (https://www.adamsandreese.com/news-knowledge/seven-points-to-know-in-new-cyberinsurance-guidance-that-help-companies-and-insurers). 26.02.2021).***

***

«Агентство национальной безопасности (АНБ) и Microsoft выступают за модель безопасности Zero Trust как на более эффективный способ защиты предприятий от современных все более изощренных угроз.

Эта концепция существует некоторое время и основана на предположении, что злоумышленник уже может быть в сети, поэтому локальным устройствам и соединениям никогда не следует доверять неявно, а проверка всегда необходима.

Компании, занимающиеся кибербезопасностью, годами продвигали модель сети с нулевым доверием как переход от традиционной системы безопасности, которая учитывала только внешние угрозы.

Модель была создана в 2010 году Джоном Киндервагом, который также ввел термин «нулевое доверие», главным аналитиком Forrester Research в то время, но разговоры о ней начались в начале 2000-х годов. Google внедрил концепции безопасности с нулевым доверием после операции «Аврора» в 2009 году для внутреннего проекта, получившего название BeyondCorp.

Защита с нулевым доверием для критически важных сетей

Недавняя атака на цепочку поставок SolarWinds, которую также приписывают государственному субъекту, возобновила дискуссию о преимуществах архитектуры безопасности с нулевым доверием для уязвимых сетей.

Президент Microsoft Брэд Смит выступал за модель нулевого доверия в своих показаниях в Сенате США относительно кибератаки SolarWinds, заявив, что эта концепция - лучший подход для организации или агентства к обеспечению безопасности идентификации в своих сетях.

Говоря о безопасности правительственных сетей США, подвергшихся атаке, Смит сказал: «Основные методы кибергигиены и безопасности не применялись с регулярностью и дисциплиной, которых мы ожидали бы от федеральных клиентов с профилями безопасности агентств. В большинстве случаев многофакторная аутентификация, наименее привилегированный доступ и другие требования для установления Среда «нулевого доверия» отсутствовала. Наш опыт и данные убедительно показывают, что если бы эти шаги были выполнены, злоумышленник имел бы лишь ограниченный успех в компрометации ценных данных даже после получения доступа к средам агентства», - Брэд Смит, президент Microsoft

Теперь и АНБ, и Microsoft рекомендуют модель безопасности с нулевым доверием для критически важных сетей (системы национальной безопасности, министерство обороны, оборонная промышленная база) и крупных предприятий.

Zero Trust - долгосрочный проект

Руководящими принципами этой концепции являются постоянная проверка аутентификации или авторизации пользователя, наименее привилегированный

доступ и сегментированный доступ на основе сети, пользователя, устройства и приложения…

АНБ поясняет, что понимание и контроль того, как пользователи, процессы и устройства взаимодействуют с данными, является фундаментальной целью Zero Trust.

Чтобы составить точную картину активности в сети, оценить ее легитимность и предотвратить горизонтальное перемещение злоумышленника, требуется несколько точек данных.

Объединение данных пользователя и устройства с важной для безопасности информацией, такой как местоположение, время, зарегистрированное поведение, может использоваться системой для разрешения или запрета доступа к определенным активам, и решение регистрируется для использования в будущей аналитике подозрительной активности. Этот процесс применяется к каждому отдельному запросу доступа к конфиденциальному ресурсу.

Однако создание зрелой среды с нулевым доверием - это не задача, которую можно решить в одночасье, а постепенный переход, который часто требует дополнительных возможностей, поскольку не учитывает новые инструменты, тактики или методы противника.

«Zero Trust включает комплексный мониторинг безопасности; детальный контроль доступа на основе рисков; и автоматизация безопасности системы скоординированным образом по всем аспектам инфраструктуры, чтобы сосредоточить внимание на защите критически важных активов (данных) в реальном времени в динамической среде угроз» - Агентство национальной безопасности

Хорошая новость заключается в том, что переход может быть постепенным и снижает риск на каждом этапе, значительно улучшая видимость и автоматические ответы с течением времени.

Преимущества сети Zero Trust

Чтобы продемонстрировать преимущества сети Zero Trust, АНБ приводит три примера, основанные на реальных инцидентах кибербезопасности, когда злоумышленник не смог бы добиться успеха, если бы концепция была реализована.

В первом случае субъект получил доступ к сети организации-жертвы с неавторизованного устройства, используя законные учетные данные, украденные у сотрудника, - уровень аутентификации, достаточный в традиционной среде безопасности.

Во втором примере злоумышленник является либо внутренней угрозой, либо субъектом, взломавшим «устройство пользователя с помощью эксплойта мобильного кода в Интернете».

В типичной среде субъект может перечислять сеть, повышать привилегии и перемещаться по сети, чтобы добиться устойчивости или найти ценные данные и системы.

Третий пример от АНБ - это атака на цепочку поставок, когда субъект добавляет вредоносный код к «популярному сетевому устройству или приложению предприятия», которое организация-жертва поддерживает и регулярно обновляет в соответствии с передовыми методами.

В архитектуре с нулевым доверием скомпрометированное устройство или приложение не сможет взаимодействовать с злоумышленником, поскольку по умолчанию ему не будет доверять.

«Его привилегии и доступ к данным будут жестко контролироваться, минимизироваться и отслеживаться; сегментация (макро и микро) будет обеспечиваться политикой; и аналитика будет использоваться для отслеживания аномальной активности. Кроме того, хотя устройство может иметь возможность загружать подписанные обновления приложений (злонамеренные или нет), разрешенные сетевые подключения устройства в рамках схемы с нулевым доверием будут использовать политику безопасности запрета по умолчанию, поэтому любая попытка подключения к другим удаленным адресам для управления и контроля, скорее всего, будут заблокированы «Агентство национальной безопасности (АНБ)

Агентство признает, что помимо технических проблем, возникающих в результате реорганизации существующей информационной системы на основе модели нулевого доверия, сопротивление всей организации может стать еще одним препятствием, снижающим эффективность системы.

Пользователи, администраторы и высшее руководство должны придерживаться одного и того же мышления, чтобы Zero Trust работала. То есть лидеры должны тратить ресурсы на его создание и поддержку, сетевые администраторы и защитники должны обладать необходимым опытом, а пользователи не должны иметь возможности обходить политики.

«После того, как в сеть будут интегрированы даже базовые или промежуточные возможности нулевого доверия, для достижения зрелости внедрения и получения всех преимуществ необходимо выполнить дополнительные действия», - говорится в сообщении NSA.

В настоящее время агентство работает с клиентами DoD над созданием систем Zero Trust и координирует деятельность с текущими программами NSS и DoD.

Готовится дополнительное руководство, чтобы упростить внедрение принципов Zero Trust в корпоративные сети. Организации, желающие принять эту концепцию, также могут найти документацию и методологию от NIST, а также от нескольких компаний, занимающихся кибербезопасностью, некоторые из которых предлагают решения для более простого внедрения». ***(Ionut Ilascu. NSA, Microsoft promote a Zero Trust approach to cybersecurity // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/nsa-microsoft-promote-a-zero-trust-approach-to-cybersecurity/). 27.02.2021).***

***

«Весной 2020 года под руководством исполнительного директора Грега Рэттрея была сформирована вторая Нью-Йоркская кибер-целевая группа (NYCTF), в которую вошли ключевые высокопоставленные члены и ведущие эксперты для анализа степени готовности США к будущей кибернетической безопасности проблемы, включая политические, экономические и

технологические разработки; изменение динамики киберконфликтов; и пандемия COVID-19.

Теперь NYCTF выпустила свой новый отчет «Повышение готовности к национальной киберзащите за счет оперативного сотрудничества» со Школой международных и общественных отношений Колумбийского университета (SIPA), в котором раскрывается готовность США к киберреагированию на вызовы национальной безопасности в киберпространстве. В своем отчете NYCTF представила суровые, но правдоподобные сценарии, намеченные на 2025 год, чтобы проверить, насколько хорошо нация сможет защитить себя в киберпространстве. Заглядывая в будущее, NYCTF отошла от вчерашних проблем и сосредоточилась на более долгосрочной кибер-готовности.

Эксперты NYCTF определили движущие силы киберрисков, в том числе геополитическую конкуренцию великих держав, достижения в новых технологиях, таких как AI и IoT, а также киберпреступников, использующих распространение передовых киберинструментов.

В своем отчете NYCTF детализирует рекомендации по созданию эффективного общенационального подхода для повышения кибер-готовности за счет оперативного сотрудничества. По сути, эти рекомендации сосредоточены на создании государственно-частной сети уполномоченных узлов для обеспечения эффективного кризисного реагирования на стратегические непредвиденные ситуации в киберпространстве. NYCTF рассматривает развитие этой сети как фундаментальный шаг в повышении готовности к киберпространству.

Эрика Боргхард - член NYCTF; Старший научный сотрудник, New American Engagement Initiative, Scowcroft Center for Strategy and Security, Atlantic Council, говорит: «Важным вкладом New York Cyber Task Force было тестирование некоторых основных рекомендаций Комиссии по киберпространству солярия, особенно тех, которые ориентированы на общественность. - частное сотрудничество. Тот факт, что в ходе тщательного процесса целевой группы были утверждены эти рекомендации, только еще больше усиливает критическую важность улучшения работы правительства США с частным сектором в отношении общих киберугроз. Это также демонстрирует безотлагательность назначения национального кибердиректора и расширения прав и возможностей эта должность должна быть координационным центром в рамках федерального правительства для сотрудничества с частным сектором».

Эксперты NYCTF надеются использовать импульс, созданный включением ключевых мер оперативного сотрудничества в недавний отчет Комиссии по соляриям и Закон о разрешении на национальную оборону 2021 года (NDAA), а также действия, предпринятые на государственном и муниципальном уровнях, а также частными лицами. сектор. Эксперты считают, что Соединенные Штаты должны предпринять целенаправленные и срочные меры по обеспечению кибер-готовности за счет улучшения оперативного сотрудничества уже сейчас.

Майкл Дэниел - член NYCTF; Президент и главный исполнительный директор Cyber Threat Alliance заявляет: «По мере того, как цифровая зависимость нашего общества продолжает расти, киберугрозы, с которыми мы сталкиваемся, также становятся все более опасными и разрушительными. Реагирование на эти

усиленные угрозы требует от нас внедрения не только новых технологий, но и новых структур, организаций, взаимоотношений и политики на всех уровнях правительства. Второй отчет New York Cyber Task Force излагает четкую серию шагов по развитию тех структур и взаимоотношений, которые заметно улучшили бы нашу кибербезопасность как нацию».

Чтобы узнать больше об отчете и основных выводах, журнал Security поговорил с Грегом Рэттреем - исполнительным директором NYCTF и соучредителем / партнером Next Peak…» ***(Maria Henriquez. New York Cyber Task Force launches report revealing national cybersecurity response readiness // BNP Media (https://www.securitymagazine.com/articles/94699-new-york-cyber-task-force-launches-report-revealing-national-cybersecurity-response-readiness). 26.02.2021).***

***

Країни ЄС та Великобританія

«Новый независимый орган будет контролировать обучение и стандарты в индустрии кибербезопасности Великобритании, приводя сектор в соответствие с другими профессиями, включая право, медицину и инженерию.

Совет по кибербезопасности Великобритании призван предоставить отрасли единый правительственный голос и помочь улучшить перспективы трудоустройства для специалистов по информационной безопасности с любым уровнем опыта, работая с поставщиками услуг по обучению для аккредитации курсов и квалификаций, а также предоставляя работодателям информацию, необходимую для эффективно нанимать сотрудников для обеспечения их безопасности.

Он направлен на улучшение перспектив трудоустройства по всей стране, давая начинающим и уже имеющимся работникам четкую дорожную карту для построения карьеры в области кибербезопасности. Совет также сосредоточится на увеличении разнообразия людей, делающих карьеру в отрасли.

Этот орган, финансируемый Департаментом цифровых технологий, культуры, СМИ и спорта (DCMS), будет работать в тесном сотрудничестве с Национальным центром кибербезопасности (NCSC) и нацелен на то, чтобы быть «универсальным магазином» для людей, которые хотят войти или продолжить свои карьера в сфере информационной безопасности.

«Кибербезопасность - это растущая отрасль в Великобритании, и жизненно важно, чтобы высокие стандарты практики и технических знаний были в основе профессии по мере ее развития», - сказал Крис Энсор, заместитель директора NCSC по развитию киберпространства.

«Мы надеемся на сотрудничество с Советом, чтобы помочь будущим поколениям профессионалов в области кибербезопасности обладать навыками и поддержкой, которые им необходимы для процветания и превращения Великобритании в самое безопасное место для жизни и работы в Интернете».

Создание Совета по кибербезопасности Великобритании произошло после консультации по развитию профессии в области кибербезопасности в

Великобритании, которая обнаружила поддержку создания нового отраслевого органа. Его возглавит Клаудия Натансон, которая работала в качестве руководителя службы безопасности в DWP и управляющим директором в BT Secure Business Service.

«Проведя много лет в сфере кибербезопасности, я хорошо осведомлен об отличной работе, проделанной многими различными организациями, но я также осознаю, что пришло время для создания зонтичной организации, чтобы единым образом продвигать профессию вперед, "сказал Натансон.

«Быть частью руководства Совета - это привилегия и вызов, зная, что будущая безопасность и процветание Великобритании частично зависит от успеха Совета в выполнении своей миссии по развитию профессии», - добавила она.

Совет официально начнет свою работу 31 марта и назначил первый попечительский совет, который будет помогать организации в ближайшие годы». ***(Danny Palmer. Cybersecurity jobs: This new 'one-stop shop' aims to create a roadmap for security careers // ZDNet (https://www.zdnet.com/article/cybersecurity-jobs-this-new-one-stop-shop-aims-to-create-a-roadmap-for-security-careers/). 09.02.2021).***

***

«Королевский университет Белфаста был назван одним из первых академических центров передового опыта в области кибербезопасности в Великобритании (ACE-CSE).

Национальный центр кибербезопасности (NCSC), входящий в состав GCHQ, наградил университет серебряным признаком своей программы ACE-CSE после того, как компания Queen's продемонстрировала, что она обеспечивает первоклассное образование в области кибербезопасности в кампусе и продвигает кибер-навыки в своем сообществе.

Северная Ирландия ставит амбициозную цель - увеличить к 2030 году количество специалистов по кибербезопасности в регионе до 5000, и мы надеемся, что эта награда поддержит усилия Университета по продолжению создания сильного потока высококвалифицированных выпускников.

Программа ACE-CSE, разработанная NCSC и Департаментом цифровых технологий, культуры, СМИ и спорта, направлена на развитие влиятельного и растущего сообщества преподавателей кибербезопасности, формирование и поддержку образования в области кибербезопасности и взаимодействие с промышленностью, правительством, преподавателями и студентами.

С момента своего основания в 2009 году Центр безопасных информационных технологий (CSIT) в Queen's приобрел прочную национальную и международную репутацию в области исследований и сотрудничества в области кибербезопасности. Он был признан одним из первых академических центров исследований в области кибербезопасности GCHQ в 2011 году.

Крис Энсор, заместитель директора NCSC по развитию кибербезопасности, сказал: «Я рад, что теперь мы можем признать первый транш университетов в качестве академических центров передового опыта в области образования в области кибербезопасности, дополняя наши существующие программы, которые

признают высококачественные исследования в области кибербезопасности и курсы повышения квалификации.

«Это свидетельство постоянных усилий ученых, вспомогательного персонала и высшего руководства, что кибербезопасность остается в их повестке дня.

«Мы очень надеемся на сотрудничество с ними в ближайшие годы и настоятельно призываем другие университеты работать над достижением аналогичного признания в будущем».

Профессор Ян Грир, президент и вице-канцлер Queen's, сказал: «Я приветствую признание Queen's NCSC в качестве одного из первых академических центров передового опыта в области образования в области кибербезопасности, подчеркивая нашу приверженность распространению знаний и знаний в области кибербезопасности во всем образовании. пути, области деятельности учреждения и более широкое сообщество. Я поздравляю команду ACE-CSE во главе с доктором Сандрой Скотт-Хейворд, которая добилась этого признания».

Queen's вложила значительные средства в персонал, инфраструктуру, стипендии и стипендии для поддержки образования и исследований в области кибербезопасности.

Д-р Сандра Скотт-Хейворд, директор ACE-CSE университета, сказала: «Мы рады, что ACE-CSE признает силу образования в области кибербезопасности и продвижение кибербезопасности прямо во всей компании Queen. Это осуществляется разнообразной командой ученых и сотрудников профессиональных служб, поддерживающих различные дисциплины. У нас есть захватывающие планы по дальнейшему развитию осведомленности и знаний о кибербезопасности в компании Queen's и за ее пределами, что, по нашему мнению, имеет фундаментальное значение для решения социальной проблемы кибербезопасности».

Дэвид Крозье, заместитель директора ACE-CSE, сказал, что Queen's стремится развивать кибер-навыки в Северной Ирландии.

Он добавил: «Северная Ирландия ставит амбициозную цель - увеличить к 2030 году число профессионалов в области кибербезопасности в регионе до 5000. Это признание ACE-CSE для Queen's поможет нам и в дальнейшем наращивать поток талантов для этой стратегически важной для региона отрасли и нация. Он также основывается на предыдущих успехах CSIT в том, что он был признан одним из первых ACE-CSR и получил степень магистра в области прикладной кибербезопасности, также сертифицированную NCSC». ***(ACE-CSE recognition for Queen's University's cyber security education // Newswise (https://www.newswise.com/articles/ace-cse-recognition-for-queen-s-university-s-cyber-security-education). 10.02.2021).***

***

«Агентство Европейского Союза по кибербезопасности (ENISA) и Объединенный исследовательский центр Европейской комиссии (JRC) выпустили совместное руководство «Проблемы кибербезопасности при обновлении искусственного интеллекта при автономном вождении».

Ключевые моменты

Поскольку автономные транспортные средства используют ИИ для многих аспектов, которые традиционно выполняются водителями-людьми, классического подхода «защиты цифровых систем» недостаточно. Вы должны рассматривать вопросы, связанные с ИИ, в контексте всей цепочки поставок, участвующей в их разработке и интеграции с другими автомобильными системами.

Искусственный интеллект и машинное обучение являются краеугольным камнем умных автомобилей с широким набором аксессуаров и станут ключом к автомобилям следующего поколения.

Наиболее значительные и известные уязвимости и возможные сценарии атак на модели искусственного интеллекта, используемые в антивирусных программах, связаны с методами компьютерного зрения.

Ключевой проблемой является правильная обработка крайних случаев, когда встречается неизвестная ситуация за пределами распределения обучающих данных: например, игнорирование знака остановки, частично покрытого снегом.

В отчете анализируются распространенные уязвимости ИИ в автономных транспортных средствах и рекомендации по их устранению». ***(Odia Kagan. Groups Outline Cybersecurity Risks for AI in Autonomous Vehicles // Fox Rothschild (https://dataprivacy.foxrothschild.com/2021/02/articles/general-privacy-data-security-news-developments/groups-outline-cybersecurity-risks-for-ai-in-autonomous-vehicles/). 15.02.2021).***

***

«После кибератак, в результате которых две больницы во Франции превратились в «полностью бумажные» в последние дни, Эммануэль Макрон подтвердил в четверг, 18 февраля, план на 1 миллиард евро для усиления кибербезопасности чувствительных систем.

В четверг утром глава государства в течение часа слушал по видеоконференцсвязи врачи и руководители больниц в Даксе и Вильфранш-сюр-Соне, рассказывая ему, как хакеры полностью парализовали их учреждение 8 и 15 февраля. Карты пациентов, телефонная связь, хирургическое оборудование, прием лекарств, записи на прием, размещение койки и врача… все было заблокировано. Письменные заметки, сделанные вручную схемы обслуживания и записные книжки каким-то образом взяли верх, но операции были незапланированными, и пациентов отправляли в другие больницы.

С тех пор команды из Ансси (Национальное агентство безопасности информационных систем) на месте пытались восстановить работоспособные компьютерные сети и восстановить данные, часть из которых была защищена в виде резервных копий. Для восстановления нормальной функции, вероятно, потребуются недели.

«Экосистема безопасности»

Руководство планирует выделить 1 миллиард евро, включая 720 миллионов государственных средств, на укрепление сектора, утроение его оборота до 25 миллиардов евро в 2025 году и удвоение численности персонала. «Многие актеры подвергаются нападениям каждый день и требуют выкупа, не говоря об этом», -

сказал Эммануэль Макрон. То, через что вы прошли, показывает как нашу уязвимость, так и важность активизации и инвестиций. "

Больницы, как и все администрации, имеют «строгие инструкции никогда не платить» выкуп, напомнил в среду в Елисейском университете, в то время как в 2020 году число этих атак увеличилось в четыре раза, и они были нацелены на 11% больниц. В разгар пандемии эти атаки представляют собой «кризис в кризисе», - отметил Глава государства. Он приветствовал предстоящее создание «кибер-кампуса» в Ла-Дефанс с участием примерно шестидесяти основных государственных и частных игроков в этом секторе, которые должны создать «экосистему безопасности, более единую и более эффективную».

По словам Гийома Пупара, директора Anssi, сетей, запускающих атаки программ-вымогателей, всего десять, напоминая о недавних успехах в Украине против сетей Emotet и Egregor, благодаря международному сотрудничеству полиции и при активном участии». ***(Cyberattaques : Emmanuel Macron promet un plan de 1 milliard d'euros après le piratage de deux hôpitaux // LeMonde (https://www.lemonde.fr/pixels/article/2021/02/18/cyberattaques-macron-promet-un-plan-de-1-milliard-d-euros-apres-le-piratage-de-deux-hopitaux_6070421_4408996.html). 18.02.2021).***

***

«В последние месяцы 2020 года Европейская комиссия продемонстрировала впечатляющую законодательную активность, поскольку она выдвинула предложения по нескольким нормативным актам (а именно Закон о регулировании данных, Закон о цифровых услугах и Закон о цифровых рынках), а также предложила новые стандартные договорные положения для международная передача данных (ожидается, что она будет принята к апрелю 2021 года), а также рассмотрела проблемы, влияющие на передачу данных в Великобританию в связи с Brexit. Среди всего этого было бы легко пропустить очень важное обновление в области кибербезопасности - предложение о Директиве о мерах по обеспечению высокого общего уровня кибербезопасности во всем Союзе (Директива NIS2), представленное 16 декабря 2020 года.

Фактически, это предложение поступило как раз вовремя, по словам директора Европейской комиссии по кибербезопасности Лорены Бойс Алонсо. Учитывая недавнюю кибератаку SolarWinds, она утверждает, что Директива NIS2 станет очень необходимым инструментом для решения критических проблем с аналогичными инцидентами в будущем, в том числе для государственных учреждений и проверки безопасности цепочки поставок.

Коротко о директиве NIS2

В случае принятия Директива NIS2 введет новые и более строгие обязательства для компаний по обеспечению адекватной кибер-готовности и реагирования. К ним относятся внедрение специализированных политик и программ обеспечения готовности к кибербезопасности и реагирования, проведение регулярных тренингов для персонала и аудит цепочки поставок, а также уведомление о любых киберинцидентах в течение всего 24 часов. Надзорные

органы также будут иметь новые правоприменительные полномочия, такие как право запрашивать информацию и проводить аудит, и даже временно препятствовать осуществлению компанией своих деловых операций и отстранять ее генерального директора за неспособность устранить выявленные недостатки.

Новая директива также привлечет больше компаний к сфере регулирования кибербезопасности ЕС. Некоторые компании, работающие в секторе наук о жизни, поставщики цифровых услуг, производители электроники и автомобилей и даже органы государственного управления относятся к числу тех, на которые в настоящее время все еще не распространяется эта система. Кроме того, директива, аналогичная GDPR, будет иметь экстерриториальную сферу действия, что означает, что компании, не входящие в ЕС, которые предоставляют услуги в ЕС, должны будут соблюдать новые правила.

Принятие институтами ЕС Директивы NIS2 ожидается к началу 2022 года, а ее внедрение в законы государств-членов ЕС - к середине 2023 года.

Учитывая быстро растущее значение кибербезопасности и связанные с этим риски, компании уже должны начать планирование директивы NIS2. Самое главное, компании должны предпринять следующие шаги:

Подумайте, насколько вероятно, что они подпадут под действие Директивы NIS2.

Определите, каков их текущий уровень зрелости кибербезопасности и в какой степени он будет считаться совместимым с Директивой NIS2.

Заранее выделяйте человеческие и финансовые ресурсы для реализации любых необходимых мер кибербезопасности

Реорганизация и оптимизация программ обеспечения готовности к кибербезопасности и реагирования (т. Е. Определение способов создания единой политики реагирования на киберинциденты и отчетности, которая соответствует требованиям GDPR и NIS2)

Историческое прошлое

В 2016 году вступила в силу Директива NIS (Директива 2016/1148 о мерах по обеспечению высокого общего уровня безопасности сетей и информационных систем в рамках Союза), которая установила первую законодательную базу, направленную на обеспечение высокого уровня кибербезопасности в ЕС.. Государства-члены должны были перенести директиву в свои национальные правовые системы к 2018 году.

Среди положений, регулирующих национальные киберстратегии, а также практику сотрудничества и обмена информацией между властями государств-членов, был также установлен ряд общих обязательств для компаний, считающихся операторами основных услуг. К ним относятся:

внедрение соответствующих и соразмерных технических и организационных мер для управления рисками, связанными с безопасностью сети и информационных систем, которые они используют в своей деятельности

предотвращение и минимизация воздействия инцидентов, влияющих на безопасность их сети и информационных систем

уведомление обо всех инцидентах, оказывающих значительное влияние на их сеть и информационные системы

Однако вскоре после начала своего действия Директива NIS уже доказала свои ограничения. Предлагаемая Директива NIS2 направлена на обновление и добавление к существующим правилам кибербезопасности, применимым к компаниям, путем:

расширение круга типов компаний, подпадающих под такие правила

требование, чтобы компании сами определяли, подпадают ли они под действие таких правил

добавление новых и более строгих обязательств для компаний и предоставление более широких правоприменительных полномочий компетентным органам

Новинки, предложенные Директивой NIS2

Больше типов организаций, подпадающих под новые правила кибербезопасности

Текущая Директива NIS применяется к операторам основных услуг, а также (в меньшей степени) к некоторым ограниченным категориям поставщиков цифровых услуг. OES определяются как организации, которые: а) предоставляют услуги, необходимые для поддержания критически важной социальной и / или экономической деятельности; б) предоставление этой услуги зависит от сети и информационных систем; и с) инцидент будет иметь серьезные разрушительные последствия для предоставления этой услуги. Однако Директива NIS ограничивает назначение OES только определенными секторами, такими как энергетика, транспорт и питьевое водоснабжение.

В связи с быстрым ростом зависимости общества от сетевых и информационных систем и все более серьезными рисками, связанными с такой тенденцией, вскоре стало ясно, что гораздо больше компаний подходят под определение OES, но работают в секторах, выходящих за рамки Директивы NIS. Таким образом, чтобы исправить этот недостаток и достичь цели высокого уровня кибербезопасности в ЕС, Директива NIS2 значительно расширит список компаний, подпадающих под действие правил кибербезопасности, включая, среди многих других, производителей и исследователей медицинские продукты и устройства, производители транспортных средств и электрических продуктов и компонентов, практически все поставщики цифровых услуг (например, платформы социальных сетей, поставщики облачных решений, центры обработки данных, службы обмена сообщениями, сети доставки контента и другие),

Все компании, подпадающие под действие Директивы NIS2, будут классифицироваться как существенные или важные организации. Это различие, хотя и с использованием разных названий, по существу аналогично тому, которое уже используется в Директиве NIS. А именно, в случае существенных субъектов, компетентные органы будут активно контролировать их соблюдение применимых правил и будут проводить проверки или другие следственные действия на регулярной основе (так называемое «предварительное исполнение»). Принимая во внимание, что для важных организаций власти будут расследовать любые потенциальные нарушения правил, если произойдет киберинцидент или появятся другие доказательства, указывающие на какие-либо недостатки в уровне

соблюдения компанией (так называемое принудительное применение «постфактум»).

Применимость Директивы NIS2 определяется компаниями, а не властями

Еще одна важная проблема Директивы NIS заключалась в том, что она возлагала бремя определения компаний, подпадающих под действие правил кибербезопасности, на органы государств-членов, а не на сами компании. Это привело к несоответствиям между государствами-членами, где часто одна и та же компания определялась как подпадающая под действие директивы в одной стране ЕС, но не в других. Это вызвало путаницу как у компаний, так и у властей, особенно в случаях, когда трансграничный инцидент затронул несколько стран с разными взглядами на классификацию компании.

Директива NIS2 решает эту проблему, перекладывая это бремя на сами компании и обязывая их идентифицировать себя как существенную или важную организацию и предоставлять необходимую информацию в этом отношении в указанный реестр. В случае, если организация не может идентифицировать себя, компетентный орган может принять меры для исправления этой ситуации, которые могут включать денежные санкции.

Новые и более строгие обязательства для компаний

В дополнение к единому общему обязательству в Директиве NIS по внедрению достаточных технических и организационных мер, Директива NIS2 потребует от компаний принятия различных других мер для обеспечения надлежащего уровня кибербезопасности. Это повлечет за собой принятие индивидуальных политик безопасности, охватывающих несколько конкретных областей риска, проведение регулярных тренингов для персонала и проверку уровней безопасности цепочек поставок компании.

Директива NIS2 также установит более подробную процедуру сообщения о киберинцидентах. Наиболее важным элементом в этом отношении будет обязанность предоставить первоначальное уведомление компетентному органу в течение 24 часов после инцидента. Это гораздо более сжатые сроки по сравнению с 72-часовым сроком, предусмотренным в GDPR. Кроме того, киберинцидент в значении этой директивы является гораздо более широким понятием, чем нарушение данных в соответствии с GDPR. Это означает, что в некоторых случаях компаниям может потребоваться сообщить об одном и том же инциденте, влияющем на личные данные, в два разных органа в течение двух разных периодов времени, а в других случаях - сообщить об инцидентах, когда личные данные не были затронуты, и обязанности по отчетности GDPR не будут применяться.

Расширение правоприменительных полномочий надзорных органов

Правоприменительные полномочия компетентных органов в соответствии с Директивой NIS2 также будут расширены и уточнены. Таким образом, органы власти будут иметь такие права, как проводить проверки на местах и аудиты безопасности, запрашивать информацию и получать доступ к данным и документам компании, издавать обязательные приказы для исправления любых недостатков, информировать общественность о неспособности компании обеспечить кибербезопасность, и назначить сотрудника по мониторингу для

надзора за соблюдением компанией требований в течение определенного периода времени.

Пожалуй, наиболее ошеломляющим дополнением к арсеналу оружия властей, введенным в Директиве NIS2, является право временно прекратить коммерческую деятельность компании и даже отстранить от должности генерального директора компании или человека, выполняющего аналогичную управленческую роль. Эти полномочия, однако, будут зарезервированы только за существенными организациями и только в тех случаях, когда компания грубо игнорирует первоначальные инструкции властей о том, как исправить любые недостатки.

Еще один аспект, который компании должны учитывать, заключается в том, что в соответствии с действующей Директивой NIS, обеспечение соблюдения осуществляется на местном уровне органами, назначенными каждым государством-членом. Кроме того, некоторые государства-члены (например, Италия и Нидерланды) назначили несколько органов, которые несут ответственность за исполнение закона только в определенном секторе бизнеса. Не похоже, что Директива NIS2 помешает государствам-членам сохранить свои первоначально назначенные органы. Таким образом, компаниям, подпадающим под действие системы кибербезопасности, необходимо будет с осторожностью сообщать о киберинцидентах во всех затронутых государствах-членах, а также сообщать о них соответствующему органу.

Экстерриториальный охват Директивы NIS2

Компании, учрежденные за пределами ЕС, но предлагающие свои услуги в пределах ЕС, также должны будут соблюдать будущую Директиву NIS2. Это означает, что если такая компания, не входящая в ЕС, классифицируется как существенная или важная организация по смыслу директивы, ей необходимо будет полностью соблюдать эту директиву (которая включает в себя все правила, описанные выше), а также назначить представитель по крайней мере в одном государстве-члене ЕС, где предлагаются его услуги.

Сроки принятия и переноса в законы государств-членов

По сравнению с постановлением, процесс принятия директивы в учреждениях ЕС обычно несколько быстрее. Тем не менее, ожидается, что Директива NIS2 будет принята не раньше начала 2022 года. После этого директива по-прежнему даст государствам-членам 18 месяцев на то, чтобы перенести ее положения в национальное законодательство. Соответственно, новые правила кибербезопасности начнут применяться не раньше середины 2023 года.

Что это значит для компаний?

Если будет принята Директива NIS2, соблюдение строгих правил кибербезопасности, требующих реализации целостной программы осведомленности и реагирования, станет скорее нормой, чем исключением. Вскоре большинство компаний, деятельность которых зависит от сетей и информационных систем и которые считаются важными или важными для общества, будут охвачены рамками кибербезопасности ЕС.

Учитывая широкие правила и риски правоприменения, предлагаемые Директивой NIS2, включая штрафы до 10 миллионов евро или 2% от глобального оборота компании, компаниям уже следует подумать о принятии определенных

шагов для подготовки. Некоторые хорошие предложения могут включать определение того, будет ли ваша компания подпадать под действие Директивы NIS2, и, если да, заранее выделить человеческие и финансовые ресурсы для обновления ваших киберпрограмм для обеспечения соблюдения. Общие юрисконсульты должны проинформировать о последствиях, с которыми может столкнуться правление компании из-за потенциального несоблюдения новых правил, выдвинуть любые предложения по смягчению таких последствий и согласовать любые необходимые бюджетные планы.

Свяжитесь со своим обычным контактным лицом Cooley, если вы хотите узнать, как лучше всего подготовиться к Директиве NIS2. Мы помогли нескольким компаниям в их усилиях по соблюдению действующей Директивы NIS и можем проконсультировать нас по поводу влияния Директивы NIS2 на ваш бизнес». ***(Enrique Gallego Capdevila, Anrijs Simkus, Patrick Van Eecke. European Commission Proposes Stricter, More Encompassing Cybersecurity Obligations for Companies // Cooley (https://cdp.cooley.com/european-commission-proposes-stricter-more-encompassing-cybersecurity-obligations-for-companies/). 25.02.2021).***

***

«Американская компания Palantir, занимающаяся данными и наблюдением, получила привилегированный доступ к высокопоставленным правительственным чиновникам Великобритании в течение нескольких месяцев, прежде чем заключить контракты на сумму более 40 миллионов фунтов стерлингов на помощь властям в их ответных мерах на коронавирус.

Внимание, проявленное к скандальной компании высокопоставленным государственным служащим торгового департамента, а также высшими должностными лицами Национальной службы здравоохранения, возможно, помогло Palantir быстро обеспечить прибыльную работу в правительстве, когда кризис впервые ударил. Его контракты с правительством Великобритании включают двухлетний контракт с NHS на создание программной платформы для обработки данных пациентов на сумму 23,5 миллиона фунтов стерлингов. Эта сделка сейчас является предметом судебного процесса в связи с предполагаемой неспособностью правительства обеспечить надлежащую защиту медицинской информации.

«Правительство имеет юридическую обязанность консультироваться с нами, гражданами и пользователями NHS, прежде чем они заключают крупные сделки... Они не сделали этого для хранилища данных Palantir: вот почему мы возбуждаем это дело», - написала Мэри Фицджеральд, редактор. -главный OpenDemocracy и Кори Крайдер, директор-основатель неправительственной организации Foxglove, которая выступает за честные технологии, в статье, объясняющей мотивацию иска.

Доступ, которым пользовался Palantir, мог дать компании «значительное преимущество» по сравнению с другими фирмами, сказал высокопоставленный член отдела закупок NHS - органа, который контролирует закупки для службы здравоохранения, - который отказался назвать свое имя. «У других компаний не было такой возможности встретиться с этими людьми и повлиять на исход важного контракта».

По словам чиновника, ставить под сомнение процесс закупок важно, потому что платформа данных играет ключевую роль в работе NHS. Они добавили, что уже существует «массовая зависимость от него во всей Национальной службе здравоохранения», «его невероятно сложно заменить».

Правительство Великобритании уже получило резкую критику за приостановку нормального надзора за внешними подрядчиками и отказ от проведения тендера на разработку, связанную с коронавирусом. Министры утверждают, что нужно было действовать быстро и не допускать задержек.

Но один специалист по глобальным государственным закупкам сказал, что процесс, ведущий к заключению контракта, «отклоняется» от золотого стандарта государственных закупок в том смысле, что «вы не должны отдавать предпочтение одной организации с дополнительной информацией или дополнительным доступом по сравнению с другими».

Когда вы «объединяете» деятельность торгового отдела «с присуждением неконкурентных контрактов, вы получаете ситуацию, в которой совершенно ясно, что если бы я был одним из конкурентов Palantir... я был бы очень, очень обеспокоен этой деятельностью», - добавил специалист.

Представитель правительства отверг эту характеристику, заявив, что это «стандартная практика» для должностных лиц торгового департамента «взаимодействовать с широким кругом предприятий в рамках их ответственности по поддержке торговли и инвестиций Великобритании», добавив: «Неверно говорить, что отдел вышел за рамки своей компетенции».

Представитель NHS сказал: «Компания является аккредитованным поставщиком для государственного сектора Великобритании, NHS завершила оценку воздействия на защиту данных в апреле 2020 года, и обновление будет опубликовано в должное время».

Palantir отказался от комментариев.

Встречает и приветствует

Palantir был соучредителем в 2014 году соучредителем PayPal, миллиардером, советником кампании Дональда Трампа и финансовым спонсором в 2016 году Питером Тилем. Документы, просочившиеся информатором АНБ Эдвардом Сноуденом, показали, что Palantir приложил руку к созданию навязчивых возможностей глобального наблюдения Агентства национальной безопасности США. Программное обеспечение фирмы также использовалось администрацией Трампа для нацеливания на иммигрантов и облегчения депортации.

Его работа с британской системой здравоохранения была первоначально стимулирована встречей в апреле 2019 года между Департаментом международной торговли (DIT), тогдашним вторым по должности государственным служащим Антонией Ромео, и Луи Мосли из Palantir, исполнительным вице-президентом и главой британского управления.

Во время встречи Ромео рассказал Мосли о NHSX - новой «совместной организации по цифровым технологиям, данным и технологиям», которая использует новые технологии и данные для оказания британской медицинской помощи, созданной в этом месяце. Встреча описана в информационных записках, подготовленных DIT и получена POLITICO через запрос свободы информации.

После встречи в апреле 2019 года Ромео связал Мозли с Дэвидом Прайором, председателем NHS England, который позже убедился, что Мэтью Гулд, генеральный директор NHSX, был вовлечен в их разговор.

По данным Бюро журналистских расследований, ко 2 июля 2019 года Прайор пил арбузные коктейли с Мосли на ужине, который босс Palantir устроил накануне запуска NHSX.

В тот же день Palantir был добавлен в качестве поставщика в утвержденный правительством список подрядчиков по облачным технологиям, сообщил представитель британского государственного органа по закупкам контрактов Crown Commercial Service (CCS).

Через несколько месяцев после ужина последовала серия встреч с Прайором, Гулдом и DIT. Затем 14 января 2020 года Приор посетил штаб-квартиру Palantir в Сан-Франциско, где он увидел демонстрацию программного обеспечения компании Palantir Foundry для здравоохранения.

Мосли снова встретился с Ромео неделю спустя, 22 января, в павильоне Palantir на ежегодном Всемирном экономическом форуме 2020 года в Давосе, Швейцария. В информационных записках Ромео говорилось, что она должна ухаживать за ним, продвигая Великобританию как лидера в области технологий и «отличное место для Palantir для расширения своего программного бизнеса» и связав его с директором по технологиям в Crown Commercial Service.

Согласно информационным бюллетеням, подготовленным для встречи в Давосе, компания рассматривает Великобританию как «ворота в остальной мир».

Сразу после январской встречи личный секретарь Ромео написал Мозли по электронной почте, чтобы познакомить его с представителями здравоохранения DIT, включая руководство DIT по наукам о жизни и директора по инвестициям.

К марту 2020 года пандемия COVID-19 была в самом разгаре, и Национальная служба здравоохранения объявила, что программное обеспечение Palantir станет частью системы реагирования на пандемию в стране с контрактом на чрезвычайную ситуацию.

«В борьбе с этой пандемией лицам, принимающим решения, потребуется точная информация в режиме реального времени», - заявил глава NHSX Гулд в своем блоге. Система, разработанная Palantir, писал он, будет собирать огромные объемы данных со всей службы здравоохранения, чтобы создать «надежную операционную картину вируса, как он распространяется, где он может распространиться дальше и как это повлияет на NHS и социальные сети». услуги по уходу». Сейчас он также используется при внедрении вакцины против COVID-19.

После нескольких контрактов, которые не были поставлены на конкуренцию к суду программного обеспечения и установить на службу, Palantir объявил о подписании нового, два года, £ 23500000 NHS контракт на правительство, чтобы использовать его в конце прошлого года». ***(GRAHAM LANKTREE. UK government accused of favorable treatment for data firm Palantir // POLITICO (https://www.politico.eu/article/uk-government-accused-of-favorable-treatment-for-data-firm-palantir/). 25.02.2021).***

***

«Как сообщает «Коммерсантъ», в нынешнем году многим государственным органам придется потратить несколько сотен миллионов рублей на доработку своих информационных систем из-за прекращения поддержки браузера Internet Explorer американской корпорацией Microsoft. Дело в том, что большинство государственных информационных систем использовали для входа пользователей устаревшую версию браузера.

После прекращения поддержки Internet Explorer системы продолжат работать, но если они не будут получать обновления, это сделает их уязвимыми для хакерских атак. Речь идёт, к примеру, про систему контроля над объёмом оборота алкогольной и спиртосодержащей продукции в России (ЕГАИС), систему Федерального казначейства (ГАС «Управление») и Верховного суда (ГАС «Правосудие»). В указанных ведомствах не ответили на запросы издания.

Все перечисленные информационные системы работают только в браузере Internet Explorer на операционной системе Windows. Когда они создавались, только Internet Explorer поддерживал необходимые требования по криптографической защите. Но с тех пор прошло много лет: Microsoft прекратит поддержку Internet Explorer версии 11 с 17 августа 2021 года, а поддержка более старых версий прекращена ещё с 12 января 2016 года.

Отсутствие обновлений несёт серьезный риск утечки данных и доступности сервисов, считают эксперты. Это повышает риск хакерских атак и сужает круг потенциальных пользователей. Проблема носит масштабный характер — для её решения потребуется переписывать программное обеспечение государственных информационных систем, на что уйдёт от одного до трёх лет, а стоить это будет сотни миллионов рублей». ***(Александр Пономарёв. Информационные системы российских органов власти могут стать уязвимы для хакеров. Из-за Internet Explorer // ООО «Фэшн Пресс» (https://www.popmech.ru/technologies/news-674243-informacionnye-sistemy-rossiyskih-organov-vlasti-mogut-stat-uyazvimy-dlya-hakerov-iz-za-internet-explorer/). 19.02.2021).***

***

«Министерство обороны Австралии выпустило новый отчет о своих выводах о том, как снизить этический риск проектов искусственного интеллекта, отметив, что смягчение киберпреступлений будет ключом к поддержанию доверия и целостности автономных систем.

Отчет был составлен с учетом опасений Министерства обороны по поводу того, что несвоевременное внедрение новых технологий может нанести военный ущерб, в то время как преждевременное внедрение без достаточных исследований и анализа может привести к непреднамеренному ущербу.

«Требуется значительная работа, чтобы гарантировать, что внедрение технологии не приведет к неблагоприятным результатам», - говорится в отчете Министерства обороны США [PDF].

Отчет является кульминацией семинара, проведенного два года назад, на котором организации, в том числе министерство обороны, другие правительственные учреждения Австралии, Центр совместных исследований в области надежных автономных систем, университеты и компании оборонной промышленности собрались вместе, чтобы изучить, как лучше всего разработать этический ИИ в контексте защиты.

В отчете участники совместно выделили пять ключевых факторов - доверие, ответственность, управление, закон, прослеживаемость - которые, по их мнению, необходимы при разработке любого проекта этичного ИИ.

Объясняя эти пять соображений, участники семинара заявили, что все проекты защиты от ИИ должны иметь возможность защищаться от кибератак в связи с глобальным ростом кибервозможностей.

«Системы должны быть устойчивыми или способны защищаться от атак, в том числе защищать свои каналы связи», - говорится в отчете.

«Способность контролировать системы была продемонстрирована на коммерческих транспортных средствах, в том числе на тех, для которых по-прежнему требуются водители, но есть подключение к «Интернету вещей». В худшем случае системы могут быть переданы на работу от имени противостоящих сторон. сил».

Участники семинара добавили, что существует риск того, что недостаток инвестиций в суверенный ИИ может повлиять на способность Австралии достичь превосходства суверенных решений.

Таким образом, участники рекомендовали повысить уровень раннего обучения ИИ для военнослужащих, чтобы улучшить способность защиты действовать ответственно при работе с ИИ.

«Без раннего обучения ИИ военнослужащих они, скорее всего, не смогут управлять ИИ, руководить им или взаимодействовать с ним, который они не могут понять и, следовательно, не могут доверять», - говорится в отчете. «Проактивные этические и правовые рамки могут помочь обеспечить справедливую подотчетность людей в системах искусственного интеллекта, гарантируя, что операторы или отдельные лица не будут подвергаться непропорциональному наказанию за общесистемное и многоуровневое принятие решений».

В отчете также одобряются инвестиции в кибербезопасность, разведку, безопасность границ и управление идентификацией, поддержку расследований и криминалистику, а также в системы ИИ, которые будут развертываться только после демонстрации эффективности посредством экспериментов, моделирования или ограниченных живых испытаний.

Кроме того, в отчете рекомендуется уделять приоритетное внимание проектам оборонного ИИ интеграции с уже существующими системами. Он предоставил пример автоматизации автомобильного транспорта, поскольку он обеспечивает уведомления о столкновениях, мониторинг слепых зон, среди прочего, которые поддерживают когнитивные функции человека-водителя.

Члены семинара также создали три инструмента, которые были разработаны для поддержки руководителей проектов ИИ в управлении этическими рисками.

Первые два инструмента - это контрольный список этической защиты от ИИ и матрица этических рисков ИИ, которые можно найти на веб-сайте Министерства обороны.

Между тем, третий инструмент - это оценка этического риска для программ искусственного интеллекта, которые требуют более полного юридического и этического плана программы. Маркированный как План программы обеспечения правовой и этической безопасности (LEAPP), оценка требует, чтобы менеджеры проектов ИИ описали, как они будут соответствовать требованиям Содружества по обеспечению правовых и этических гарантий.

LEAPP требует, чтобы менеджеры проектов AI создали документ с информацией, такой как юридическое и этическое планирование, прогресс и оценка рисков, а также данные для внутреннего планирования Defence, включая обзоры вооружений. После того, как эта оценка будет написана, она будет отправлена на рассмотрение и комментарий заинтересованным сторонам оборонного сектора и промышленности, прежде чем она будет рассмотрена для заключения оборонных контрактов.

Поскольку выводы и инструменты из отчета являются лишь рекомендациями, в нем не уточняется, какие проекты защиты от ИИ подходят для оценки LEAPP». ***(Campbell Kwan. Defence lists cyber mitigation as key factor for building ethical AI // ZDNet (https://www.zdnet.com/article/defence-lists-cyber-mitigation-as-key-factor-for-building-ethical-ai/). 17.02.2021).***

***

«Amazon Web Services (AWS) обратился с просьбой о внедрении механизма, который может предоставить поставщикам онлайн-аккаунтов иммунитет при ответе на ордера на захват аккаунта, выданные некоторыми правоохранительными органами Австралии.

Появление такого механизма следует из Поправки в Surveillance Законодательство Билл 2020, которая была внесена в Парламент, и, если она будет принята, то потребует передачи 3 ордеров австралийской федеральной полиции (AFP) и новой австралийской криминальной разведывательной комиссия (ACIC) рычагов для борьбы с преступностью в Интернете.

Первый ордер - это ордер на нарушение данных, который, согласно пояснительной записке к законопроекту, предназначен для использования для предотвращения «продолжения преступной деятельности участниками и является наиболее безопасным и наиболее целесообразным вариантом, когда эти участники находятся в неизвестных местах или действуют анонимно или подают ложные данные».

Второй - это ордер на сетевую активность, который позволит AFP и ACIC собирать информацию об устройствах, которые используются или могут быть использованы теми, на кого распространяется ордер.

Последний ордер - это ордер на захват учетной записи, который позволит агентствам взять под свой контроль учетную запись с целью блокировки лица из этой учетной записи.

В AWS заявили, что первый и третий ордера «сформулированы для принципиально разных целей правоохранительных органов по сравнению с ордерами, которые правоохранительные органы могут запрашивать в настоящее время».

«Эти два ордера предназначены не для сбора доказательств как таковых, а для того, чтобы позволить сотрудникам правоохранительных органов эффективно выступать в роли (онлайн) лиц, подозреваемых в причастности к потенциальной преступной деятельности», - говорится в сообщении [PDF] в Объединенный парламентский комитет по разведке и безопасности в рамках рассмотрения законопроекта.

«Хотя оба эти ордера являются дополнительными по отношению к существующим ордерам, они являются существенным отходом от текущих положений, и их выдача повлечет за собой повышенный риск для свободы и конфиденциальности граждан, чьи онлайн-аккаунты подвергаются влиянию правоохранительных органов».

AWS считает, что исполнение ордеров правоохранительными органами или добросовестное оказание помощи сотрудникам правоохранительных органов, исполняющим ордер, не должно приводить к гражданской ответственности перед лицом.

В нем говорилось, что для ордеров на захват учетной записи и помощи, предоставляемой в соответствии с распоряжениями о помощи, относящимися к ордерам на захват учетной записи, должно быть положение, защищающее третьи стороны от ответственности.

«AWS заявляет, что в закон следует внести поправки, чтобы ввести новый иммунитет для поставщиков онлайн-аккаунтов в отношении исполнения ордеров на захват аккаунтов», - говорится в сообщении.

«Иммунитет должен распространяться на уголовную и гражданскую ответственность или действие или другую форму судебного разбирательства о возмещении ущерба в связи с действием или бездействием, совершенным добросовестно при предполагаемом соблюдении или во исполнение требования в соответствии с захватом счета. ордер».

AWS также обеспокоена тем, что новые ордера могут вынудить облачного гиганта внедрить системные недостатки или уязвимости в свои системы.

AWS подняла аналогичные вопросы несколько лет назад, ранее заявляя, что положения Закона 2018 года о телекоммуникациях и другом законодательстве (помощь и доступ) могут потребовать действий, которые могут сделать технологические системы менее безопасными.

В конечном итоге в Закон были включены положения, в которых перечислялись вопросы, которые лица, принимающие решения, должны учитывать при определении того, были ли уведомления об обращении за помощью в отрасли в соответствии с этим Законом разумными и соразмерными.

К последнему законопроекту он потребовал добавить аналогичные соображения и отдельно рассмотреть техническую осуществимость для тех, кто выдаёт ордера.

«Кроме того, AWS утверждает, что исполнение ордеров, предложенных в законопроекте, не должно приводить к появлению системных недостатков или уязвимостей в любой форме электронной защиты данных, реализованной в системах поставщика технологий», - говорится в сообщении.

«Такой ордер был бы неразумным при любых обстоятельствах, поскольку он создал бы значительный и длительный риск для невиновных третьих лиц».

Другой запрос AWS заключается в том, что, учитывая потенциальное пересечение законодательных положений в отношении обращения за помощью, законопроект должен использовать критерии Закона о помощи и доступе для определения того, что является «разумным и соразмерным».

«На наш взгляд, законопроект в нынешнем виде не обеспечивает достаточной защиты для отдельных сотрудников поставщиков технологий, таких как облачные сервисы, и создает режим помощи, отличный от того, который предусмотрен для поставщиков технологий в соответствии с Законом о помощи и доступе», - AWS написал.

«Законопроект позволяет правоохранительным органам запрашивать ордер на оказание помощи, требующий от определенного лица предоставить любую информацию или помощь, которая является разумной и необходимой для исполнения ордера. Указанное лицо включает сотрудника владельца или арендатора компьютера или нанятого лица по договору об оказании услуг владельцем или арендатором компьютера, либо лицом, которое является или было системным администратором системы, включая компьютер».

Он сказал, что эти определения могут включать сотрудников поставщика облачных услуг.

AWS также обеспокоен тем, что сотрудники, которым может быть приказано совершить действие или вещь или не выполнить действие или вещь в соответствии с приказом о помощи, могут затем быть принуждены к нарушению иностранного закона или побудить другое лицо к нарушению иностранного закона.

В результате он попросил, чтобы в законопроекте было ясно, что любое такое требование было бы необоснованным или обеспечивало бы защиту для человека, который отказывается совершить действие или совершить бездействие». ***(Asha Barbaschow. AWS asks new Australian computer warrant provide immunity for account takeovers // ZDNet (https://www.zdnet.com/article/aws-asks-new-australian-computer-warrant-provide-immunity-for-account-takeovers/). 15.02.2021).***

***

«Исследователи рекомендовали правительству Австралии отказаться от существующей системы цифровой идентификации и начать заново с нуля, снова подчеркнув недостатки безопасности в двух уже аккредитованных системах.

Профессор Ванесса Тиг и Бен Френгли в прошлом году сообщили Налоговому управлению Австралии (ATO) о слабости его системы myGovID. Они

обнаружили, что myGovID подвержен легко реализуемой атаке с проксированием кода, которая позволяет вредоносному веб-сайту проксировать логин myGovID человека и повторно использовать его аутентификацию для входа в учетную запись жертвы на любом веб-сайте по своему выбору.

Пара сообщила, что ATO в ответ проинформировала их о том, что у них нет намерений исправлять ошибку.

Агентство цифровой трансформации (DTA) отвечает за Trusted Digital Identity Framework (TDIF), которая представляет собой высокоуровневый дизайн для федеративной системы аутентификации.

«Основная цель безопасности механизма аутентификации состоит в том, чтобы помешать злоумышленникам мошенническим образом войти в чужие учетные записи. Вторичная цель безопасности - сохранить конфиденциальность документов, удостоверяющих личность, и биометрических данных, используемых для установления личности», - пишут исследователи [PDF].

«Ни дизайн высокого уровня TDIF, ни его реализация ATO (myGovID) не соответствуют поставленным целям безопасности».

myGovID является аккредитованным поставщиком цифровых удостоверений, как и аналогичная служба идентификации почты Австралии. Тиг и Френгли также выявили недостатки в системе почтовой службы.

По словам исследователей, Identity Exchange (IdX) выступает в качестве единой точки отказа как для конфиденциальности, так и для аутентификации, что приводит к «чрезвычайно хрупкой архитектуре, которая допускала бы крупномасштабное мошенничество с идентификацией, если бы этот компонент перешел под контроль злонамеренная партия».

Они сказали, что IdX предназначен для сокрытия личности проверяющей стороны от поставщика удостоверений, но не может этого сделать в реализации ATO. Обеспокоенность обоих вызывает то, что реализация TDIF в Digital iD Почты Австралии, похоже, даже не использует IdX, который является фундаментальным компонентом конструкции TDIF.

«Хотя мы не исследовали подробно реализацию Australia Post, кажется, что она существенно отличается от спецификации TDIF, но, по-видимому, все равно была аккредитована», - добавили они.

«TDIF в том виде, в каком он разработан и внедрен в настоящее время, не соответствует его собственным руководящим принципам - не сразу очевидно, что модель с посредничеством без технических средств для сохранения конфиденциальности даже может им соответствовать».

В результате исследователи рекомендовали «тщательную переоценку приоритетов TDIF» и рассмотрение других вариантов, которые могут соответствовать его целям.

Альтернативы, предложенные парой, включают использование системы на основе инфраструктуры открытого ключа или использование простого, стандартного, попарного протокола OpenID Connect вместо «сложной модели посредничества с плохими свойствами конфиденциальности и безопасности».

«От системы следует отказаться и заново разработать ее с нуля людьми, имеющими некоторое представление о конструкции безопасного протокола и

некоторыми заботами о защите своих сограждан от кражи личных данных», - написали они.

«Законодательство, обеспечивающее безопасность с помощью указов, не помешает организованной преступности, иностранным правительствам или обычным преступникам воспользоваться недостатками его конструкции. Инфраструктура открытых ключей имеет гораздо больше шансов на успех».

Исследователи также были обеспокоены параграфом в консультативном документе DTA, в котором говорится, что итоговое законодательство о цифровых идентификаторах будет включать дополнительные механизмы, включая штрафы за защиту информации, используемой в системе, такой как биометрическая информация.

Эти механизмы могут включать положения об уголовных преступлениях и положениях о гражданском наказании.

«Существует множество австралийских законов, которые эффективно наказывают защиту информации, но мы впервые видим, что цель четко сформулирована без ссылки на террористов или педофилов», - написали Тиг и Френгли.

"Мы надеемся, что это опечатка, и настоятельно рекомендуем вместо этого наказать за несоответствующий обмен или небрежную утечку информации.

«Важно не криминализировать исследования в области безопасности, направленные на повышение безопасности системы, путем открытого изучения ее (многочисленных, серьезных) слабых мест». ***(Asha Barbaschow. Researchers want Australia's digital ID system thrown out and redesigned from scratch // ZDNet (https://www.zdnet.com/article/researchers-want-australias-digital-id-system-thrown-out-and-redesigned-from-scratch/). 16.02.2021).***

***

Інші країни

«Согласно новому исследованию восприятия рисков кибербезопасности в Латинской Америке с начала кризиса, большинство бразильских компаний не увеличили свои инвестиции в информационную и кибербезопасность с момента возникновения пандемии Covid-19, несмотря на рост угроз.

Согласно опросу, проведенному консалтинговой фирмой Marsh от имени Microsoft, 84% организаций не смогли увеличить свои расходы на безопасность с марта 2020 года, хотя 30% опрошенных отметили рост вредоносных атак в результате нового коронавируса. кризис, причем наиболее частыми случаями являются фишинг и вредоносное ПО.

Несмотря на рост угроз безопасности, 56% опрошенных бразильских компаний в настоящее время инвестируют 10% или меньше своего ИТ-бюджета в кибербезопасность. Согласно исследованию, 52% бразильских организаций заявили, что объем инвестиций в безопасность не изменился с начала пандемии.

Что касается практики сотрудников в области безопасности, только 23% бразильских организаций, принявших участие в исследовании, заявили, что их

сотрудники используют для работы оборудование, предоставленное компанией. На региональном уровне 70% латинских организаций разрешили своим сотрудникам использовать свои личные устройства после перехода на удаленную работу.

Согласно исследованию, это значительно повысило подверженность киберинцидентам того или иного типа, но безопасность удаленного доступа является приоритетом только для 12% респондентов и вторым пунктом в списке для 7% респондентов.

Только четверть опрошенных латинских компаний увеличили свои бюджеты на кибербезопасность после пандемии, в то время как увеличение бюджета на защиту данных составило 26%. Более того, только 17% организаций в Латинской Америке имеют страховку от киберугроз.

«Многие результаты этого анализа действительно вызывают беспокойство, например, низкие ставки компаний, имеющих страховку от киберрисков и инвестиции в безопасность», - сказала Марта Шу, суперинтендант по киберрискам в Marsh Brazil.

«Теперь, когда компании более подвержены удаленной работе и использованию личных устройств, вызывает беспокойство тот факт, что немногие компании увеличили свой бюджет на кибербезопасность после пандемии, а некоторые даже сократили эти инвестиции, несмотря на заметное увеличение числа кибератак», - добавила она. Исследование следует за новостями о массовых утечках данных в Бразилии, которые произошли в последние недели». ***(Angelica Mari. Brazilian firms fail to increase security spend through Covid-19 // ZDNet (https://www.zdnet.com/article/brazilian-firms-fail-to-increase-security-spend-through-covid-19/). 20.02.2021).***

***

«Сингапур выделяет 24 миллиарда сингапурских долларов (18,1 миллиарда долларов) в течение следующих трех лет, чтобы помочь местным предприятиям внедрять инновации и создавать возможности, необходимые для проведения следующего этапа преобразований. Финансовый импульс будет направлен на различные инициативы, такие как Программа новых технологий, в рамках которой правительство софинансирует расходы на испытания и внедрение новых технологий, включая 5G, искусственный интеллект (ИИ) и кибербезопасность.

Это было необходимо для того, чтобы страна оставалась конкурентоспособной и была готова использовать будущие возможности, сказал заместитель премьер-министра и министр финансов Хенг Сви Кит во время своей парламентской речи во вторник, подробно описывая бюджет Сингапура на 2021 финансовый год. Он отметил, что прошлогодняя серия бюджетов была наклонена в сторону «экстренная поддержка» в свете глобальной пандемии, но необходимо было сосредоточить инвестиции в этом году на ускорение «структурной адаптации».

Он указал на меняющуюся конкурентную среду, вызванную быстротой технологического прогресса и реконфигурацией глобальных цепочек поставок, как

на ключевой фактор, побуждающий все заинтересованные стороны действовать и быстро реагировать, чтобы использовать различные возможности.

Хэн сказал: «Мы должны перейти от антициклической политики фискальной и денежно-кредитной стабилизации к структурной экономической политике, чтобы снабдить наши предприятия и наших сотрудников глубокими и готовыми к будущему возможностями».

В этом аспекте правительство будет стремиться к развитию бизнес-сообщества, «обладающего сильным духом новаторства» и имеющего «глубокую связь» с Азией и миром. По его словам, будет также предоставлен определенный капитал для поддержки бизнеса в их преобразовании и расширении.

Это будет включать корпоративную площадку для запуска предприятий, которая будет предлагать компаниям софинансирование для создания новых предприятий через предварительно отобранные венчурные студии. Министр пояснил, что новая платформа, пилотная версия которой запланирована на этот год, будет актуальна для крупных предприятий, стремящихся развивать в своей организации стартап-мышление.

BCG Digital Ventures, например, представляет собой венчурную студию, которая в партнерстве с местной продовольственной и сельскохозяйственной компанией Olam разработала Jiva, платформу фермерских услуг, призванную помочь фермерам увеличить урожайность и напрямую связаться с потенциальными покупателями.

Также разрабатываются планы по расширению Открытой платформы инноваций с помощью новых функций, позволяющих связать компании и государственные учреждения с соответствующими поставщиками технологий для решения их бизнес-задач. Например, облачный цифровой стенд поможет облегчить создание и тестирование виртуальных прототипов, сказал Хенг.

Он добавил, что платформа открытых инноваций также предлагает совместное финансирование прототипирования и развертывания. Управление строительства и строительства, например, было согласовано с тремя поставщиками технологий - TraceSafe, TagBox и Nervotec - для разработки инструментов, обеспечивающих безопасное открытие рабочих мест. К ним относятся системы в реальном времени, которые позволили владельцам строительных площадок отслеживать контакты с COVID-19 и контролировать состояние здоровья своих сотрудников.

Также будут внесены улучшения в Глобальный инновационный альянс, который был создан в 2017 году для облегчения трансграничного партнерства между Сингапуром и глобальными инновационными центрами. По словам Хэна, с момента его запуска более 650 студентов и 780 сингапурских компаний приняли участие в запусках инноваций за рубежом, из которых 40% находились в Юго-Восточной Азии.

Он сказал, что инвестиции будут по-прежнему направляться на расширение партнерства и создание инфраструктуры в регионе Asean, отметив, что сильная связь имеет важное значение для того, чтобы предприятия Сингапура могли подключаться к глобальным и региональным цепочкам поставок и отраслевым кластерам.

По словам Хэна, страны АСЕАН в совокупности были пятой по величине экономикой мира, генерировав ВВП в 3,2 триллиона долларов в 2019 году, и в прошлом году стали крупнейшим торговым партнером Китая. Обладая значительным потенциалом роста в регионе, он сказал, что Сингапур продолжит работу с членами Asean для улучшения цифровой связи и кибербезопасности, а также для дальнейшего продвижения таких инициатив, как Asean Smart Cities Network.

К ним относятся усилия по созданию кластера отраслей, связанных с медициной, производством продуктов питания и электроникой, спрос на которые в Asean растет. Он сказал, что недавно был создан Производственный альянс Юго-Восточной Азии для поддержки таких усилий с целью продвижения сети промышленных парков для производителей, которые хотят инвестировать в Сингапур и регион.

Чтобы еще больше стимулировать сингапурские компании, включая крупные, малые и средние предприятия, инвестировать в новые технологии для повышения своей конкурентоспособности, правительство заявило, что оно также будет софинансировать внедрение цифровых инструментов и новых технологий.

Говоря о программе Emerging Technology Program, Хенг сказал, что эта инициатива снизит затраты на испытания и развертывание таких технологий, как 5G, AI и «доверенные» технологии, а также поддержит коммерциализацию инноваций.

По его словам, новая программа цифровых лидеров также поддержит компании в процессе найма их основных цифровых команд и в разработке и развертывании стратегий цифровой трансформации.

Министр добавил, что правительство будет сотрудничать с акционерными обществами, чтобы предложить местным предприятиям капитал для трансформации и масштабирования. Здесь 500 миллионов сингапурских долларов будут совместно инвестированы с государственной инвестиционной фирмой Temasek Holdings в Платформу финансирования местных предприятий, которая будет управляться на коммерческой основе. Кроме того, Temasek будет соответствовать государственным инвестициям, предоставив в общей сложности 1 миллиард сингапурских долларов, сказал он.

Подчеркивая необходимость подготовки лидеров инноваций и предприятий, особенно в областях глубоких технологий, правительство Сингапура также учредит новую программу стипендий в области инноваций и предприятий. По словам Хэна, в течение следующих пяти лет программа будет поддерживать 500 стипендий.

Эта инициатива, возглавляемая Национальным исследовательским фондом (NRF), направлена на удовлетворение требований в таких областях, как кибербезопасность, искусственный интеллект и медицинские технологии, и NRF будет работать с различными партнерами, включая акселераторы, фирмы венчурного капитала и стартапы в области глубоких технологий, для создания программы. вверх.

БОЛЬШОЙ УСПЕХ НА ЗЕЛЕНОМ

Поскольку изменение климата «реально и безотлагательно», также были выделены средства для поддержки зеленых инициатив Сингапура. На прошлой

неделе страна представила свой «Зеленый план 2030» - десятилетний план, направленный на стимулирование усилий по созданию «зеленого, пригодного для жизни и устойчивого» дома для будущих поколений.

По словам Хэна, технологии играют здесь ключевую роль и откроют новые возможности, поскольку они уже помогли Сингапуру решить проблему водных и земельных ограничений.

Среди его целей - планы по развертыванию 60 000 точек зарядки электромобилей на общественных парковках и в частных помещениях к 2030 году, а также инвестиции в размере 30 миллионов сингапурских долларов в течение следующих пяти лет для инициатив, связанных с электромобилями.

Правительство также определило экологические проекты государственного сектора на сумму до 19 миллиардов сингапурских долларов, включая инициативу Tuas Nexus, которая будет финансироваться за счет зеленых облигаций. По словам Хэна, проект объединяет очистные сооружения для сточных вод и воды, а также оптимизирует восстановление энергии и ресурсов в процессах очистки твердых отходов и использованной воды». ***(Eileen Yu. Singapore puts budget focus on transformation, innovation // ZDNet (https://www.zdnet.com/article/singapore-puts-budget-focus-on-transformation-innovation/). 16.02.2021).***

***

«Фонд Electronic Frontier Foundation (EFF) призвал правительство Индонезии внести поправки в законодательство о регулировании Интернета, назвав эти законы «серьезной угрозой правам индонезийцев на свободное выражение мнений».

Законодательство о регулировании Интернета вступило в силу в ноябре прошлого года в рамках усилий по созданию нормативно-правовой базы, регулирующей управление и надзор за поставщиками электронных систем со стороны частных лиц.

Согласно международной юридической фирме Hogan Lovells, законы, которые в настоящее время доступны только на индонезийском языке Bahasa, обязывают всех операторов частных электронных систем (ESO) регистрироваться и получать удостоверение личности, выданное правительством Индонезии.

Обязательство распространяется на все частные ESO, которые управляют интернет-порталами, веб-сайтами и приложениями, которые используются для торговли, доставки контента, поисковых систем или облачных вычислений, - написал партнер Hogan Lovells Чалид Хейдер [PDF].

Отсутствие регистрации до 24 мая приведет к тому, что внутренний интернет-регулятор наложит санкции на лиц, не прошедших регистрацию, путем блокировки их услуг и контента.

Законы Индонезии также предоставляют правительству право принуждать частные ESO, за исключением поставщиков облачных услуг, удалять запрещенную информацию, в том числе контент, который создает «беспокойство для общества» и «нарушает общественный порядок».

«Это оказывает сдерживающее воздействие на свободу выражения мнений: платформы, естественно, предпочтут ошибиться в сторону удаления содержимого

серой зоны, вместо того чтобы рисковать наказанием», - говорится в сообщении EFF в блоге.

«Фактически, правительство Индонезии изучает новые минимумы в жестком, навязчивом и непрозрачном регулировании Интернета. Регламент MR5, изданный Министерством связи и информационных технологий Индонезии, направлен на усиление контроля правительства над цифровым контентом и пользователями». данные."

Частные ESO также должны назначить местное контактное лицо в Индонезии, которое будет отвечать за удаление контента или распоряжения о доступе к персональным данным.

Согласно EFF, платформам будет намного сложнее сопротивляться приказам и будет уязвима для внутренних судебных исков, включая потенциальный арест и уголовные обвинения.

В ответ на приказы о блокировке, полученные от правительства Индии, которые угрожали лишить свободы сотрудников компании, Twitter в прошлом месяце навсегда заблокировал или скрыл более 500 учетных записей на своей платформе.

В тот же день, когда EFF раскритиковал правительство Индонезии, и Google, и Reddit опубликовали обновления, в которых основное внимание уделялось влиянию скоординированных операционных кампаний по влиянию и спама, соответственно, на их платформы.

Ежеквартальный отчет группы анализа угроз Google показал, что он заблокировал почти 3000 каналов YouTube в рамках продолжающегося расследования скоординированных операций по влиянию, связанных с Китаем.

Около 3000 заблокированных каналов в основном размещали спам-контент на китайском языке о музыке, развлечениях и образе жизни, в то время как небольшая группа загружала контент на китайском и английском языках, критикующий реакцию США на COVID-19 и политические разногласия.

В обновлении прозрачности Reddit платформа показала, что удалила 85 миллионов спам-контента. Он также сообщил, что получил 611 стандартных запросов на предоставление информации о пользователях от правоохранительных органов или правительства и 324 запроса на экстренное раскрытие информации, хотя он не указал, какие типы ордеров использовались для выдачи этих запросов, и подробно описал только один такой запрос.

Этот запрос поступил от Управления электросвязи Пакистана, которое утверждало, что 812 сообществ Reddit содержат непристойные материалы и обнаженные тела, что нарушает его внутреннее уголовное законодательство в Интернете. Из этих 812 субреддитов, о которых сообщил пакистанский регулятор, платформа ограничила доступ в страну до 753 из них». ***(Campbell Kwan. Indonesian internet regulatory laws are serious threat to free expression rights: EFF // ZDNet (https://www.zdnet.com/article/indonesian-internet-regulatory-laws-are-serious-threat-to-free-expression-rights-eff/). 17.02.2021).***

***

«Правящие военные Мьянмы разработали новые законы о кибербезопасности, которые были широко осуждены как драконовские, дающие правительству широкие полномочия по доступу к данным пользователей и блокировке он лайн-сайтов. Законодательство также может подорвать положение страны как оффшорного центра предоставления услуг передачи данных, поскольку это не будет соответствовать международным законам.

Через несколько дней после военного переворота 1 февраля просочилась информация о том, что черновик законопроекта был отправлен телекоммуникационным компаниям и поставщикам онлайн-услуг для получения отзывов, которые должны быть отправлены обратно в понедельник. По мнению различных организаций, которые ознакомились с 36-страничным документом, предлагаемый закон потребует, чтобы онлайн-платформы, работающие в стране, сохраняли все данные пользователя, включая IP-адрес, домашний адрес и идентификационный номер, в течение трех лет и в системе, назначенной правительство.

Кроме того, статья 29 позволит правительству предписать перехватить, заблокировать или удалить учетную запись пользователя, если она будет выявлена как разжигающая ненависть или нарушить мир с помощью «фейковых новостей», «дезинформации или комментариев, нарушающих существующие законы. доступ к данным по запросу без ордера.

Нынешнее военное правительство, назвавшее себя Советом государственного управления, представило предлагаемый закон как необходимый для борьбы с киберпреступностью и различными действиями в Интернете, которые считаются вредными для страны.

Однако различные организации выступили с осуждением правил как репрессивных, содержащих расплывчатые термины, которые дадут правительству полномочия объявлять контент вне закона и преследовать его автора. Многие считают, что это также знаменует собой значительный шаг назад после многих лет экономического и социального прогресса в Мьянме.

В своем заявлении Центр ответственного бизнеса Мьянмы (MCRB) предупредил, что такие законы не только повлияют на гражданское общество, но и могут оттолкнуть международных инвесторов и помешать росту местного бизнеса, особенно в секторе ИКТ.

MCRB выделил акцент закона на локализации данных, требующий хранения данных на сайтах, обозначенных правительством, что, по его словам, сделает местный бизнес уязвимым. Это особенно верно для банков и компаний электронной коммерции, которые используют значительные объемы данных, поскольку они не смогут использовать безопасность и функции, предлагаемые глобальными облачными сервисами, говорится в сообщении.

Между тем, финансовые учреждения не смогут снизить риски безопасности и обеспечить управление, а это оттолкнет иностранных инвесторов и нанесет ущерб местным предприятиям, которые уже пытаются справиться с кризисом COVID-19.

Способность Мьянмы создавать рабочие места и быть центром офшорных услуг на основе данных, таких как центры обработки вызовов и общие центры

обслуживания, также будет подорвана, поскольку предлагаемый закон не будет соответствовать международным правилам защиты данных, включая Общую защиту данных ЕС. Регламент (GDPR), сказал MCRB.

Он отметил, что Федерация компьютеров Мьянмы, Ассоциация компьютерной индустрии Мьянмы и Ассоциация компьютерных специалистов Мьянмы уже высказали свои возражения против законопроекта.

Норвежская телекоммуникационная группа Telenor заявила во вторник в своем заявлении, что закон следует обсудить в парламенте и проконсультироваться с заинтересованными сторонами в отрасли, чтобы убедиться, что он «соответствует назначению» и соответствует конституции Мьянмы.

Описывая его как широкий по своему охвату, компания заявила, что предложенный закон предоставит широкие полномочия, которые могут «существенно повлиять на многих». Компания сообщила, что с 2013 года ее операции на местах были основаны на обязательствах правительства Мьянмы о том, что ее нормативно-правовая база будет соответствовать передовой международной практике. Сюда входило создание независимого регулирующего органа в сфере телекоммуникаций.

«Мы обеспокоены тем, что предлагаемый законопроект не способствует развитию соответствующей нормативно-правовой базы и закона для цифрового будущего, [также он] не способствует и не защищает цифровую безопасность и права», - заявила Telenor, добавив, что принятие законопроекта «неуместно». с такими широкими полномочиями временной администрации во время чрезвычайного положения.

Он также призвал к предложенному законопроекту обеспечить прозрачность и «правовую определенность» в отношении осуществления полномочий и исключить положения, которые могут быть использованы для упорядочивания перехвата учетных записей пользователей. Он отметил, что законы, регулирующие защиту персональных данных, электронные транзакции и кибербезопасность, должны храниться отдельно для обеспечения управления.

Называя предлагаемый закон «драконовским», Хьюман Райтс Вотч призвала к отмене законов, поскольку они «укрепят» способность правительства проводить повсеместное наблюдение и ограничат доступ к основным услугам. В законах также не указано, как власти будут определять, что считается дезинформацией, и не предусмотрено никаких вариантов для тех, чей контент был заблокирован или удален для подачи апелляции, сообщила организация.

Юрисконсульт Human Rights Watch по Азии Линда Лахдхир заявила: «Проект закона о кибербезопасности предоставит военным, только что устроившим переворот, печально известно, что критики сажают в тюрьму практически неограниченные права доступа к пользовательским данным, подвергая опасности любого, кто высказывается».

Согласно предложенным правилам компании, которые не соблюдают правила, могут быть приговорены к лишению свободы сроком до трех лет или штрафу в размере 10 миллионов кьятов (7 009 долларов США).

«Положения настоящей кибербезопасности закона представляют явную угрозу права граждан Мьянмы к достоверной информации и к конфиденциальности

журналистов и блоггеры данных,» сказала Дэниел Bastard, Азиатско-Тихоокеанский регион глава Репортеров без границ (RSF) в заявление. «Мы призываем цифровых игроков, действующих в Мьянме, начиная с Facebook, отказаться от этой шокирующей попытки подчинить их. У этой хунты нет абсолютно никакой демократической легитимности, и для платформ было бы очень разрушительно подчиняться ее тираническим установкам».

По данным RSF, у Facebook почти 25 миллионов пользователей в стране или 45% местного населения. Он добавил, что доступ к платформе социальных сетей, а также к другим, таким как Twitter и Instagram, был заблокирован вскоре после переворота 1 февраля.

UNI Global Union также призвал заинтересованные стороны отрасли выступить против закона, выделив японскую KDDI, катарскую Ooredoo и Telenor, поскольку эти три транснациональные корпорации имеют сильное присутствие в Мьянме.

Генеральный секретарь Глобального союза UNI Кристи Хоффман, представляя около 3 миллионов сотрудников в секторе услуг ИКТ, заявила: «Этот так называемый закон о кибербезопасности только защищает власть правительства и станет мощным оружием против профсоюзных деятелей, студентов, учителей и других людей. широкий круг гражданского общества высказывается. Международное сообщество должно встать, чтобы отвергнуть этот закон... Телекоммуникационные компании также должны выступить против этого закона, иначе они рискнут стать оружием этой военной хунты против демократии».

По данным группы активистов Access Now, во вторник хунта Мьянмы приказала еще раз отключить Интернет на фоне увеличения военного присутствия и применения силы против демонстрантов. В нем описывается "вооружение" отключений интернета военными, чтобы заставить замолчать инакомыслие, "неприемлемым и грубым нарушением законов о правах человека".

Директор по азиатско-тихоокеанской политике и старший международный советник Access Now Джит Сингх Чима сказал: «Законопроект Мьянмы о кибербезопасности уже вселяет страх перед слежкой и преследованием за то, что вы говорите и делаете в Интернете. возможность сообщать о государственных заказах, касающихся отключения Интернета, веб-цензуры или слежки за пользователями, вызывает большое беспокойство. Учитывая развивающуюся ситуацию и подавление бесплатных СМИ на местах, способность телекоммуникационных компаний предоставлять информацию о правительственных директивах, которые они получают, является ключевым фактором.» ***(Eileen Yu. Myanmar's proposed cybersecurity Bill draws wide condemnation // ZDNet (https://www.zdnet.com/article/myanmars-proposed-cybersecurity-bill-draws-wide-condemnation/). 16.02.2021).***

***

«Вьетнам пополнил ряды правительств, использующих шпионское ПО для борьбы с правозащитниками.

Как утверждает Лаборатория безопасности Amnesty International, правозащитники подвергаются кибератакам в рамках более широких усилий вьетнамского государства по цензуре всех, кто выступает против правительства.

Ocean Lotus, известный злоумышленник, появившийся еще в 2013 году, стоит за кампанией шпионского ПО против правозащитников и долгое время считался преследующим цели, «соответствующие интересам вьетнамского государства», согласно докладу Amnesty International о ситуации.

В докладе поясняется, что шпионское ПО - это всего лишь последний инструмент, направленный против несогласных блоггеров и активистов со стороны вьетнамского правительства, арсенал, который также включает преследования, нападения, запреты на поездки и тюремное заключение.

Цифровая цензура Вьетнама

Согласно Amnesty International, закон о кибербезопасности, принятый в 2019 году, дал правительству Ханоя полный контроль над тем, кто имеет доступ к Интернету. Но те правозащитники, которые остаются в сети, стали мишенями для атак Ocean Lotus, говорится в отчете.

Согласно расследованию Amnesty International, первые атаки шпионского ПО на правительственных диссидентов начались в феврале 2018 года.

В число мишеней входили активист демократического движения Буй Тхань Хиеу, ныне проживающий в Германии; Вьетнамская зарубежная инициатива по расширению прав и возможностей совести (VOICE) (некоммерческая организация, поддерживающая вьетнамских беженцев и права человека); и неопознанный блоггер во Вьетнаме, критикующий правительство. По словам исследователей, все они получали электронные письма со шпионским ПО в виде вложения или ссылки.

Команда Security Lab выявила шпионское ПО для операционных систем macOS и Windows.

«Шпионское ПО для Windows было разновидностью семейства вредоносных программ Kerrdown и использовалось исключительно группой Ocean Lotus», - поясняется в отчете. «Kerrdown - это загрузчик, который устанавливает дополнительное шпионское ПО с сервера в системе жертвы и открывает ложный документ».

По ссылке был загружен набор инструментов для тестирования проникновения Cobalt Strike, который дает злоумышленникам контроль над целевой системой и дает им возможность распространяться вбок.

Версия Cobalt Strike для macOS - это специальная версия вредоносного ПО, используемого только Ocean Lotus, говорится в отчете.

Amnesty International предлагает всем, кто может стать целью атак этого типа вредоносных программ, уделять пристальное внимание ссылкам, включать двухфакторную аутентификацию (2FA), использовать антивирусное программное обеспечение и запускать обновления программного обеспечения.

Кибератаки на правозащитников

Этот последний отчет - еще один пример в длинном списке государственных кампаний, организованных против правозащитников и гражданского общества.

На этой неделе тибетские сообщества стали мишенью для настроенного вредоносного расширения Firefox, чтобы обеспечить доступ и контроль

злоумышленникам, работающим с коммунистической партией Китая, по словам исследователей из Proofpoint.

А прошлым летом шпионское ПО для Android под названием ActionSpy было разослано жертвам в Тибете, Турции и Тайване с целью сбора данных об уйгурских меньшинствах, жертвах нарушений прав человека, спонсируемых Китаем.

Другие вредоносные программы, в том числе инструменты наблюдения для Android под названием SilkBean, GoldenEagle, CarbonSteal и Double-Agent, также были развернуты лицами, ориентированными на правительство Китая, в июле в рамках продолжающейся кампании слежки за мусульманами-уйгурами, которая началась еще в 2013 году.

Индустрия безопасности вместе с Amnesty International и другими группами, такими как Electronic Frontier Foundation, продолжают бить тревогу по поводу реальных последствий кибербезопасности для жизни и смерти, когда инструменты обращаются против наиболее уязвимых групп населения планеты.

«Когда мы говорим о безопасности, мы должны спросить: «Безопасность для кого?», - объяснила Ева Гальперин из EFF на сессии Black Hat 2019 года под названием «Взлом во благо: расширение возможностей технологов для укрепления цифрового общества». «Обычно это для правительств или корпораций. Мы не говорим о безопасности людей, особенно тех, у кого мало денег». ***(Becky Bracken. Cyberattacks Launch Against Vietnamese Human-Rights Activists // Threatpost (https://threatpost.com/cyberattacks-vietnam-human-rights-activists/164284/). 25.02.2021).***

***

Протидія зовнішній кібернетичній агресії

«Пресс-секретарь президента России Дмитрий Песков считает абсурдной формулировку из доклада спецслужб Франции о причастности РФ к кибератакам на предприятия этой страны.

"Да, там содержатся обвинения в неких киберпреступлениях со стороны некой группы хакеров. Безусловно, Россия не имела, не имеет и не может иметь никакой причастности к каким-либо проявлениям киберпреступности", - сказал Песков. "В этом контексте хотел бы напомнить, что именно Россия постоянно говорит о необходимости международного сотрудничества в рамках противодействия киберопасности", - заключил он.

Согласно новому отчету ANSSI, за атаками стоит известная APT-группа Sandworm, связываемая ИБ-экспертами с Россией. Жертвами вредоносной кампании преимущественно являются поставщики информационных технологий, в частности, провайдеры web-хостинга. Первая жертва была скомпрометирована в конце 2017 года, а в целом операция продолжалась до 2020 года». ***(Песков считает абсурдной формулировку о причастности России к кибератакам во Франции // SecurityLab.ru (https://www.securitylab.ru/news/516699.php). 17.02.2021).***

***

«Правительственные ведомства ОАЭ стали целями новой кампании кибершпионажа, предположительно организованной иранскими хакерами.

Как полагают исследователи безопасности из Anomali, за киберпреступной операцией стоит группировка Static Kitten (также известная как MERCURY или MuddyWater). Целью преступников является установка инструмента удаленного управления под названием ScreenConnect (теперь называется ConnectWise Control) с уникальными параметрами запуска. Вредоносные исполняемые файлы и URL-адреса, используемые в этой кампании, замаскированы под ресурсы Министерства иностранных дел Кувейта и Национального совета ОАЭ.

Специалисты обнаружили два размещенных на Onehub ZIP-файла, якобы содержащие отчет об отношениях между арабскими странами и Израилем или документ, касающийся стипендий. Атака начинается с рассылки фишинговых писем с фальшивыми документами, которые содержат URL-адреса для загрузки ZIP-фалов. В ZIP-архивах содержатся замаскированные под отчеты и документы EXE-файлы, которые при запуске начинают процесс установки ScreenConnect.

«URL-адреса, распространяемые через фишинговые электронные письма, перенаправляют получателей в место хранения файлов на легитимном сервисе Onehub, который ранее использовался Static Kitten в злонамеренных целях. Static Kitten продолжает использовать Onehub для размещения файла, содержащего ScreenConnect», — отметили исследователи.

Предположительно, конечной целью злоумышленников является использование программного обеспечения для подключения к конечным точкам в клиентских сетях, что позволяет им осуществлять дальнейшее перемещение по сети и выполнять произвольные команды в целевых средах, облегчая кражу данных.

ConnectWise Control — автономное приложение для удаленного рабочего стола с поддержкой автоматического доступа и проведения собраний с функциями совместного использования экрана». ***(Иранские хакеры используют инструмент ScreenConnect в целях кибершпионажа // SecurityLab.ru (https://www.securitylab.ru/news/516538.php). 12.02.2021).***

***

«Нідерландській економіці загрожує цифрове шпигунство з боку Китаю та Росії, через це спецслужби хочуть більшого фінансування та кращої співпраці з урядами, компаніями та університетами…

Спецслужби AIVD, MIVD та Національний координатор з питань боротьби з тероризмом та безпекою (NCTV) повідомили, що вони щодня ловлять китайських та російських хакерів, що зламують компанії та університети.

Також регулярно проводяться напади на так звану життєво важливу інфраструктуру Нідерландів, таку як об'єкти енергетики та питної води, банки та телекомунікаційні мережі.

За словами шефа MIVD Яна Свілленса, китайці та росіяни не бояться робити кібератаки: "Вони хочуть цього, можуть і роблять".

Напади на важливі елементи економіки загрожують "національній спроможності заробляти", говорить начальник AIVD Ерік Акербум.

Акербум стверджує, що небезпека з боку Китаю недооцінюється. Тому він хоче, щоб відтепер іноземні інвестиції в Нідерландах оцінювались на предмет потенційних загроз національній безпеці.

У грудні ще двох російських дипломатів було оголошено персонами нон-грата та вислано з країни після того, як AIVD викрила їх як шпигунів. Вони вишукували конфіденційну інформацію від голландських високотехнологічних компаній та установ.

Спецслужби також наголошують на потребі мати більше власних хакерів. Тому бюджет для них повинен збільшуватися. Зазначається, що у Британії та Франції нещодавно відповідні бюджети збільшили на 5 та 8 відсотків.

Щорічно AIVD отримує понад 316 мільйонів євро. Бюджет MIVD є державною таємницею». ***(Спецслужби Нідерландів вимагають більше фінансування через кібератаки Китаю і РФ // Європейська правда (https://www.eurointegration.com.ua/news/2021/02/11/7119671/). 11.02.2021).***

***

«Совет Европейского Союза на уровне министров иностранных дел определил три направления действий в отношениях с Российской Федерацией.

Об этом вице-президент Европейской Комиссии, Высокий представитель ЕС по вопросам внешней политики и безопасности Жозеп Боррель заявил на брифинге после заседания Совета Евросоюза на уровне министров иностранных дел стран-членов ЕС. (Брифинг транслировался на сайте аудиовизуальных услуг Еврокомиссии).

"В Совете ЕС считают, что Россия движется в направлении авторитарного государства и отдаляется от Европы", - подчеркнул Боррель.

В частности, по его словам, главы МИД стран-членов ЕС единодушно считают, что последние действия России и реакция свидетельствуют о четком сигнале, что она не заинтересована в сотрудничестве с Евросоюзом, а, наоборот, заинтересована в конфронтации и отстраненности от ЕС.

В связи с этим сегодня главы МИД решили следовать трем основным направлениям в отношениях с Россией.

В частности, ЕС "будет давать отпор, если Россия будет нарушать международное право и права человека".

Второе направление взаимодействия стран Евросоюза заключается в сдерживании, если Россия будет пытаться усилить давление на Евросоюз, в том числе с помощью дезинформации и кибератак, и третье – взаимодействие в вопросах, представляющих интерес ЕС…» ***(Будет давать отпор: Совет Евросоюза определил три направления действий в отношениях с РФ // УНИАН (https://www.unian.net/world/otnosheniya-es-i-rf-sovet-evrosoyuza-opredelil-tri-napravleniya-deystviy-novosti-mira-11330576.html). 22.02.2021).***

***

«В России заявили, что киберподразделения США уже находятся по всему миру, в том числе в Украине, Черногории и Северной Македонии. Об этом в четверг, 4 февраля, сообщает ТАСС со ссылкой на слова замдиректора российского Национального координационного центра по компьютерным инцидентам (НКЦКИ) Николая Мурашова.

«Под предлогом защиты выборов инфраструктурами союзников в настоящее время по всему миру разворачиваются американские киберподразделения. Согласно официальным данным военных ведомств, американские киберкоманды разместили своих специалистов на территории Черногории, Македонии, Украины», — сказал Мурашов.

По его словам, формулировка их заявлений позволяет предположить, что этот список не является полным.

Также Мурашов заявил, что киберкоманды США открыто признают, что эти подразделения обладают силами и средствами для проведения компьютерных атак, которые успешно применяются на практике против любой информационной инфраструктуры, из которой, по их мнению, исходит угроза. Также, по его словам, на территории Великобритании развернута группа по борьбе с кибермошенничеством, созданная секретной службой США.

Мурашов подчеркнул, что в задачу подразделений входит выявление, предотвращение и ликвидация последствий компьютерных атак с целью ареста и осуждения совершающих их лиц». ***(В РФ заявили, что в Украине работают киберподразделения США // Версии.com (https://versii.com/news/v-rf-zajavili-chto-v-ukraine-rabotajut-kiberpodrazdelenija-ssha/). 04.02.2021).***

***

Кібератака на SolarWinds

«Группа безопасности Microsoft заявила сегодня, что официально завершила расследование взлома, связанного с SolarWinds, и не нашла доказательств того, что хакеры злоупотребляли ее внутренними системами или официальными продуктами для разворота и атаки на конечных пользователей и бизнес-клиентов.

Производитель ОС начал расследование взлома в середине декабря после того, как было обнаружено, что хакеры, связанные с Россией, взломали поставщика программного обеспечения SolarWinds и внедрили вредоносное ПО в платформу мониторинга Orion, продукт, который Microsoft также развернула внутри компании.

В сообщении в блоге, опубликованном 31 декабря, Microsoft заявила, что обнаружила, что хакеры использовали доступ, полученный через приложение SolarWinds Orion, для перехода во внутреннюю сеть Microsoft, где они получили доступ к исходному коду нескольких внутренних проектов.

«Наш анализ показывает, что первый просмотр файла в исходном репозитории был в конце ноября и закончился, когда мы обезопасили затронутые учетные записи», - заявила компания сегодня в своем заключительном отчете о взломе, связанном с SolarWinds.

Microsoft заявила, что после перекрытия доступа злоумышленника хакеры продолжали попытки доступа к учетным записям Microsoft в течение декабря и даже до начала января 2021 года, через несколько недель после раскрытия взлома SolarWinds, и даже после того, как Microsoft дала понять, что расследуют инцидент.

«Не было случая, чтобы доступ ко всем репозиториям, относящимся к какому-либо отдельному продукту или услуге, был открыт», - заявила сегодня служба безопасности компании. «Не было доступа к подавляющему большинству исходного кода».

Вместо этого, по словам производителя ОС, злоумышленники просмотрели «только несколько отдельных файлов [...] в результате поиска в репозитории».

Microsoft заявила, что, судя по поисковым запросам, выполненным злоумышленником внутри своих репозиториев кода, злоумышленники, похоже, были сосредоточены на обнаружении секретов (также называемых токенами доступа), которые они могли использовать для расширения своего доступа к другим системам Microsoft.

Компания Redmond заявила, что эти поиски не увенчались успехом из-за внутренней практики кодирования, которая запрещала разработчикам хранить секреты внутри исходного кода.

ТАКЖЕ БЫЛ ЗАГРУЖЕН НЕКОТОРЫЙ ИСХОДНЫЙ КОД

Но помимо просмотра файлов хакерам также удалось загрузить некоторый код. Однако Microsoft заявила, что данные не были обширными и что злоумышленники загрузили только исходный код нескольких компонентов, связанных с некоторыми из ее облачных продуктов.

Согласно Microsoft, эти репозитории содержали код для:

небольшое подмножество компонентов Azure (подмножества услуг, безопасности, удостоверений)

небольшое подмножество компонентов Intune

небольшое подмножество компонентов Exchange

В целом, инцидент не привел к повреждению продуктов Microsoft или к получению хакерами обширного доступа к пользовательским данным». ***(Catalin Cimpanu. Microsoft says SolarWinds hackers downloaded some Azure, Exchange, and Intune source code // ZDNet (https://www.zdnet.com/article/microsoft-says-solarwinds-hackers-downloaded-some-azure-exchange-and-intune-source-code/). 18.02.2021).***

***

«Команда Белого дома, ведущая расследование взлома SolarWinds, обеспокоена тем, что взлом 100 американских компаний может превратить первоначальный компромисс в головную боль в будущем.

Энн Нойбергер, заместитель советника по национальной безопасности Белого дома по вопросам кибербезопасности и новых технологий, заявила на брифинге для прессы, что были взломаны девять правительственных агентств, в то время как

многие из 100 организаций частного сектора США, которые были взломаны, были технологическими компаниями.

«Многие компромиссы частного сектора связаны с технологическими компаниями, включая сети компаний, продукты которых могут быть использованы для запуска дополнительных вторжений», - сказал Нойбергер, бывший директор по кибербезопасности Агентства национальной безопасности.

Злоумышленники, которые, по утверждениям США, имеют "вероятно российское происхождение", взломали систему сборки программного обеспечения американского поставщика программного обеспечения SolarWinds и внедрили бэкдор Sunburst в его широко используемый продукт Orion для мониторинга корпоративных сетей.

То, что в результате атаки были взломаны 100 компаний частного сектора, рисует иную картину, чем то, что было известно в декабре, когда Microsoft и FireEye, которые были взломаны, раскрыли атаку.

На этом этапе было подтверждено, что были взломаны восемь федеральных агентств, в том числе Министерство финансов США, Министерство внутренней безопасности, Государственный департамент США, Министерство энергетики США и Национальное управление ядерной безопасности.

Однако в то время Microsoft и FireEye были двумя наиболее значительными компаниями частного сектора, которые, как известно, были скомпрометированы испорченным обновлением Orion (обновления Orion были не единственным способом проникновения компаний во время кампании, в которой также участвовали хакеры, получившие доступ в облачные приложения).

"Когда происходит компромисс такого масштаба и масштаба как в правительстве, так и во всем технологическом секторе США, чтобы привести к последующим вторжениям, это больше, чем единичный инцидент шпионажа. Это принципиально важно, чтобы это могло стать разрушительным, - пояснил Нойбергер во время допроса.

Она подчеркнула, что злоумышленники были «продвинутыми», потому что «уровень знаний, которые они продемонстрировали о технологии и способах ее компрометации, действительно был высоким».

«Как страна, мы выбрали как конфиденциальность, так и безопасность, поэтому разведывательное сообщество в основном не имеет доступа к сетям частного сектора. Хакеры начали взлом изнутри Соединенных Штатов, что еще больше усложнило для правительства США наблюдение за их деятельностью.," она сказала.

Президент Microsoft Брэд Смит сказал 60 Minutes на прошлой неделе, что «было бы справедливо сказать, что это самая крупная и самая изощренная атака, которую когда-либо видел мир».

Ранее Смит сказал, что злоумышленники «использовали метод, который поставил под угрозу цепочку поставок технологий для экономики в целом».

«Мы полагаем, что [злоумышленникам] потребовались месяцы, чтобы спланировать и выполнить этот взлом. Нам потребуется время, чтобы раскрыть его слой за слоем», - сказал Нойбергер.

Нойбергер сказала, что ожидает, что расследование, а также идентификация и восстановление затронутых сетей займут месяцы, но не годы». ***(Liam Tung. SolarWinds attack hit 100 companies and took months of planning, says White Hous // ZDNet (https://www.zdnet.com/article/solarwinds-attack-hit-100-companies-and-took-months-of-planning-says-white-house/). 18.02.2021).***

***

«Microsoft предоставляет открытый исходный код для запросов CodeQL, которые использовались для исследования влияния вредоносных программ Sunburst или Solarigate, установленных в обновлениях программного обеспечения SolarWinds Orion. Другие организации могут использовать запросы для выполнения аналогичного анализа.

Microsoft опубликовала запросы как часть своего ответа на атаку на программное обеспечение для мониторинга сети SolarWinds Orion, которое использовалось для выборочного взлома девяти федеральных агентств США и 100 компаний частного сектора, многие из которых были из технологического сектора.

Подозреваемые при поддержке правительства России хакеры взломали систему сборки SolarWinds в начале 2020 года, чтобы отразить атаку на цепочку поставок, обнаруженную Microsoft и FireEye - подвиг, на который, по оценкам Microsoft, потребовалось не менее 1000 инженеров.

«Ключевым аспектом атаки Solorigate является компрометация цепочки поставок, которая позволила злоумышленнику модифицировать двоичные файлы в продукте Orion SolarWinds», - говорится в сообщении службы безопасности Microsoft.

«Эти модифицированные двоичные файлы распространялись через ранее законные каналы обновления и позволяли злоумышленнику удаленно выполнять вредоносные действия, такие как кража учетных данных, повышение привилегий и горизонтальное перемещение, для кражи конфиденциальной информации. Этот инцидент напомнил организациям, что они должны задуматься не только о своей готовности для ответа на изощренные атаки, а также устойчивость собственной кодовой базы».

Microsoft использовала запросы CodeQL для анализа исходного кода и подтверждения отсутствия в исходном коде индикаторов компрометации (IoC) и шаблонов кодирования, связанных с вредоносным ПО Solorigate, также известным как Sunburst.

Ранее в этом месяце Microsoft признала, что хакеры SolarWinds загрузили некоторый исходный код Azure, Exchange и Intune в ходе ограниченной атаки. Он и FireEye были скомпрометированы испорченным обновлением Orion.

Статический и динамический анализ кода являются частью системы защиты, которую организации могут использовать для обнаружения программных атак.

Microsoft предупреждает, что результаты запросов необходимо будет пересмотреть, потому что индикаторы «могут случайно появиться в доброкачественном коде».

В нем добавлено: «Кроме того, нет гарантии, что злоумышленник ограничен той же функциональностью или стилем кодирования в других операциях, поэтому

эти запросы могут не обнаруживать другие имплантаты, которые значительно отклоняются от тактики, наблюдаемой в имплантате Solorigate».

Компания также поделилась своей философией безопасности.

«Microsoft давно использует средства контроля целостности, чтобы убедиться, что финальные скомпилированные двоичные файлы, распространяемые на наши серверы и нашим клиентам, не были злонамеренно изменены ни на одном этапе цикла разработки и выпуска. Например, мы проверяем, что хэши исходных файлов сгенерированы компилятором соответствуют исходным файлам. Тем не менее, в Microsoft мы живем в соответствии с философией «предполагать нарушение», которая говорит нам, что независимо от того, насколько усердны и обширны наши методы обеспечения безопасности, потенциальные злоумышленники могут быть столь же умны и располагать ресурсами».

Процессы сборки SolarWinds были не единственным слабым местом, которое использовали злоумышленники. На слушаниях в Сенате США на этой неделе генеральный директор CrowdStrike Джордж Курц раскритиковал Microsoft за «системные недостатки в архитектуре аутентификации Windows», сославшись на Active Directory и Azure Active Directory, сообщает Reuters. Это позволяло злоумышленникам перемещаться в сторону после компрометации сети. CrowdStrike стал целью во время атаки, но в декабре заявил, что «не пострадал».

Майк Хэнли, недавно назначенный директор по безопасности (CSO) GitHub, принадлежащего Microsoft, сказал, что CodeQL обеспечивает «ключевые ограждения, которые помогают разработчикам избегать инцидентов и уязвимостей доставки» ***(Liam Tung. Microsoft: We've open-sourced this tool we used to hunt for code by SolarWinds hackers // ZDNet (https://www.zdnet.com/article/microsoft-weve-open-sourced-this-tool-we-used-to-hunt-for-code-by-solarwinds-hackers/). 26.02.2021).***

***

Кіберзахист критичної інфраструктури

«Австралийское управление сигналов (ASD) ожидает, что вмешательство в ответ на кибератаки компаний, считающихся критически важной инфраструктурой, будет происходить только в «редких обстоятельствах».

Как описано в нынешней форме законопроекта о внесении поправок в законодательство о безопасности (критическая инфраструктура) 2020 года, государственная помощь будет предоставляться организациям в ответ на серьезные кибератаки на австралийские системы. Технологические гиганты, работающие в Австралии, такие как Amazon Web Services, Cisco, Microsoft и Salesforce, не согласны с этими полномочиями «в крайнем случае».

«В редких случаях серьезного инцидента в области кибербезопасности, влияющего на доступность ключевых объектов критически важной инфраструктуры, часть 3A, раздел 5 законопроекта обеспечивает механизм, позволяющий правительству напрямую помочь владельцу или оператору активов быстро реагировать на инциденты, связанные с кибербезопасностью, и устранять

их., "ASD объясняет в своем представлении [PDF] в Объединенный парламентский комитет по разведке и безопасности (PJCIS).

Секретарь Министерства внутренних дел может запросить ASD для оказания помощи в реагировании на серьезный инцидент кибербезопасности. Министр внутренних дел должен проконсультироваться с владельцем или оператором активов, прежде чем разрешить секретарю запросить помощь ASD, а санкционированные меры должны быть «соразмерными и технически осуществимыми».

Прежде чем вмешаться, правительство должно удостовериться в том, что инцидент кибербезопасности произошел, происходит или неизбежен; что инцидент оказывает существенное негативное влияние на функционирование критически важного объекта инфраструктуры; инцидент представляет существенный риск для социальной или экономической стабильности Австралии, ее народа, национальной обороны или национальной безопасности; соответствующая организация или организации не желают или не могут предпринять все разумные шаги для реагирования на инцидент; и никаких других вариантов практического и эффективного ответа не существует.

«Вмешательства в рамках этого положения ограничены», - сказал ASD. «При реагировании на критический киберинцидент группы реагирования на инциденты ASD смогут предпринимать только действия, указанные в разрешении министерства».

Однако это может включать в себя доступ, изменение или изменение функционирования компьютеров и реализацию мер по снижению риска, восстановление из резервных копий и установку «инструментов реагирования на инциденты».

Это также может включать доступ, восстановление, копирование, изменение или удаление программного обеспечения.

Техническое сообщество обеспокоено таким вмешательством правительства, которое подорвет цели защиты и восстановления. Microsoft, например, считает, что это приведет к возникновению «тумана войны», что еще больше усложнит любую попытку смягчить реакцию кибератак.

Проект закона, который в парламент в декабре, также вводит позитивное обязательство безопасности критически важных объектов инфраструктуры, при поддержке требований сектора конкретных требований и обязательных отчетов в ASD, а также расширенные обязательства кибербезопасности для тех субъектов условной критической инфраструктуры.

В своем заявлении ASD заявила, что ее знание внутренних угроз и уязвимостей кибербезопасности зависит от австралийского сообщества и отрасли, которые добровольно сообщают об инцидентах.

«Больше сообщений об инцидентах в ASD с помощью положений, предложенных в законопроекте, будет способствовать повышению уровня осведомленности о ситуации на национальном уровне и позволит ASD выявлять тенденции и предоставлять целевые советы другим, чтобы помочь организациям лучше подготовить и защитить свои сети и критически важную инфраструктуру Австралии.», - сказал PJCIS.

В нем говорится, что чуть более трети всех инцидентов, о которых сообщалось в Австралийский центр кибербезопасности ASD за последние 12 месяцев, были связаны с критически важными секторами инфраструктуры Австралии.

«Ожидается, что это лишь небольшая часть числа инцидентов, связанных с кибербезопасностью, затрагивающих критически важную инфраструктуру, учитывая добровольный характер отчетности», - говорится в сообщении.

Согласно предложению, как только ответственное лицо узнает об инциденте кибербезопасности, об этом должно быть сообщено в течение 12 часов, если инцидент оказывает значительное влияние на доступность актива; или 72 часа, если инцидент влияет на доступность, целостность или надежность актива или на конфиденциальность информации об активе или хранимой им информации.

«Основная цель получения ASD информации в соответствии с Частью 2B будет заключаться в улучшении национальной ситуационной осведомленности, позволяя производить анонимные рекомендации по смягчению последствий, чтобы помочь отдельным секторам или организациям в более широком смысле принять меры для защиты», - пишет ASD». ***(Asha Barbaschow. ASD says cyber attack intervention will be 'rare' under critical infrastructure Bill // ZDNet (https://www.zdnet.com/article/asd-says-cyber-attack-intervention-will-be-rare-under-critical-infrastructure-bill/). 15.02.2021).***

***

«После инцидента в Oldsmar, когда неустановленный злоумышленник получил доступ к сети водоочистных сооружений и изменил дозировку химикатов до опасных уровней, ФБР во вторник разослало предупреждение, обратив внимание на три проблемы безопасности, которые были замечены на сеть завода после взлома на прошлой неделе.

Уведомление, называемое Уведомлением частной отрасли или ПИН-кодом ФБР, предупреждает об использовании устаревших систем Windows 7, неверных паролях и программного обеспечения для совместного использования рабочего стола TeamViewer, призывая частные компании, федеральные и правительственные организации проверять внутренние сети и доступ к ним. политики соответственно.

TEAMVIEWER ПОСЧИТАЛ ТОЧКУ ВХОДА

ПИН-код ФБР специально называет TeamViewer программным обеспечением для совместного использования рабочего стола, за которым следует следить после того, как приложение было подтверждено как точка входа злоумышленника в сеть водоочистной станции Oldsmar.

Согласно сообщению Reuters, официальные лица заявили, что злоумышленник дважды подключался к компьютеру в сети водоочистной станции Oldsmar через TeamViewer в прошлую пятницу.

Во втором случае злоумышленник активно контролировал мышь оператора, перемещал ее по экрану и вносил изменения в уровни гидроксида натрия (щелока), которые добавлялись в питьевую воду.

Оператор почти сразу отменил изменения, внесенные хакером, но инцидент мгновенно стал предметом спора и обсуждения среди специалистов по безопасности.

Среди наиболее частых тем, которые поднимались в онлайн-обсуждениях, было использование приложения TeamViewer для доступа к ресурсам критически важной инфраструктуры США.

В опубликованном во вторник отчете по материнской плате несколько известных экспертов по безопасности раскритиковали компании и сотрудников, которые часто используют программное обеспечение для удаленной работы, назвав его небезопасным и неадекватным для управления конфиденциальными ресурсами.

Хотя предупреждение ФБР по PIN-коду не содержит критического тона или позиции в отношении TeamViewer, ФБР хотело бы, чтобы федеральные и частные организации приняли к сведению приложение.

«Помимо законного использования, TeamViewer позволяет киберпреступникам осуществлять удаленный контроль над компьютерными системами и передавать файлы на компьютеры-жертвы, что делает его функционально похожим на троянов удаленного доступа (RAT)», - заявило ФБР.

«Однако законное использование TeamViewer делает аномальные действия менее подозрительными для конечных пользователей и системных администраторов по сравнению с обычными RAT.

Предупреждение ФБР конкретно не сообщает организациям об удалении TeamViewer или любого другого программного обеспечения для совместного использования рабочего стола, но предупреждает, что TeamViewer и другое аналогичное программное обеспечение могут быть использованы для злоупотреблений, если злоумышленники получат доступ к учетным данным сотрудников или учетные записи удаленного доступа (например, используемые для Доступ к Windows RDP) защищены слабыми паролями.

ФБР ПРЕДУПРЕЖДАЕТ ОБ ИСПОЛЬЗОВАНИИ WINDOWS 7... СНОВА

Кроме того, предупреждение ФБР также предупреждает о продолжающемся использовании Windows 7, операционной системы, срок службы которой истек в прошлом году, 14 января 2020 года, о проблеме, о которой ФБР также предупреждало американские компании в прошлом году.

Эта часть предупреждения была включена, потому что водоочистная станция Oldsmar все еще использовала системы Windows 7 в своей сети, согласно отчету правительства Массачусетса.

Хотя нет никаких доказательств того, что злоумышленники злоупотребляли ошибками, специфичными для Windows 7, ФБР заявляет, что продолжать использовать старую операционную систему опасно, поскольку ОС не поддерживается и не получает обновлений безопасности, что в настоящее время оставляет многие системы уязвимыми для атак через недавно обнаруженные уязвимости.

Однако опубликованный сегодня отчет Cyberscoop подчеркивает тот факт, что завод Oldsmar, как и многие другие водоочистные сооружения в США, часто недофинансируется и укомплектован персоналом.

Хотя ФБР предостерегает от использования Windows 7 по уважительным причинам, многие компании, а также федеральные агентства и агентства штатов США могут быть не в состоянии что-либо с этим поделать, исключая серьезные финансовые вложения в модернизацию ИТ-инфраструктуры со стороны высшего руководства, чего не ожидается в любое время. скоро во многих местах.

В этих случаях ФБР рекомендует ряд основных передовых практик безопасности в качестве промежуточного способа смягчения угроз, таких как:

Используйте многофакторную аутентификацию;

Используйте надежные пароли для защиты учетных данных протокола удаленного рабочего стола (RDP);

Убедитесь, что антивирусные, спам-фильтры и брандмауэры обновлены, правильно настроены и безопасны;

Аудит сетевых конфигураций и изоляция компьютерных систем, которые не могут быть обновлены;

Проведите аудит вашей сети на предмет наличия систем, использующих RDP, закрытия неиспользуемых портов RDP, применения двухфакторной аутентификации, где это возможно, и регистрации попыток входа в систему RDP;

Журналы аудита для всех протоколов удаленного подключения;

Обучать пользователей выявлять попытки социальной инженерии и сообщать о них;

Выявлять и приостанавливать доступ пользователей, проявляющих необычную активность;

Обновляйте программное обеспечение». ***(Catalin Cimpanu. Following Oldsmar attack, FBI warns about using TeamViewer and Windows 7 // ZDNet (https://www.zdnet.com/article/following-oldsmar-attack-fbi-warns-about-using-teamviewer-and-windows-7/). 10.02.2021).***

***

Захист персональних даних

«RIPE NCC, организация, которая управляет и назначает адреса IPv4 и IPv6 для Европы, Ближнего Востока и бывшего Советского Союза, сегодня раскрыла неудавшуюся кибератаку на свою инфраструктуру.

«В прошлые выходные RIPE NCC Access, наша служба единого входа (SSO), пострадала от того, что, по всей видимости, было преднамеренной атакой с заполнением учетных данных, что привело к некоторому простою», - говорится в сообщении организации, размещенном ранее на ее веб-сайте. сегодня.

Агентство заявило, что смягчило атаку и обнаружило, что ни одна учетная запись не была взломана, но расследование все еще продолжается.

«Если мы обнаружим, что учетная запись была затронута в ходе нашего расследования, мы свяжемся с владельцем учетной записи индивидуально, чтобы проинформировать их».

Основанная в 1992 году, RIPE NCC в настоящее время контролирует распределение ресурсов нумерации Интернета (адресов IPv4, адресов IPv6 и номеров автономных систем) центрам обработки данных, хостинговым компаниям, операторам связи и поставщикам интернет-услуг в регионе EMEA.

Компрометация любой учетной записи RIPE NCC создаст большие проблемы как для RIPE, так и для владельцев учетных записей, поскольку это позволит злоумышленникам переназначить, даже если временно, интернет-ресурсы третьим лицам.

Адреса IPv4 в настоящее время пользуются очень высоким спросом во всем мире, и за последнее десятилетие сформировался процветающий черный рынок. Этот рынок подпитывается захваченными блоками адресов IPv4, и его наиболее частыми клиентами являются банды вредоносных программ, которые используют его для аренды доступа к захваченным адресным пространствам IPv4, чтобы они могли рассылать спам и обходить блок-списки спама.

Согласно расследованию AFRINIC, в 2019 году был обнаружен один из самых громких взломов адресного пространства IPv4, когда более 4,1 миллиона адресов IPv4 были переданы южноафриканскими компаниями новым владельцам.

У RIPE NCC официально закончились адреса IPv4 в ноябре 2019 года, что объясняет, почему злоумышленники теперь охотятся за учетными записями участников в надежде захватить существующие пулы адресов.

В настоящее время RIPE просит всех своих членов, численность которых составляет около 20 000 организаций, включить двухфакторную аутентификацию для своих учетных записей Access, чтобы предотвратить получение злоумышленниками доступа к этим ресурсам с помощью простых атак типа грубой силы». ***(Catalin Cimpanu. RIPE NCC discloses failed brute-force attack on its SSO service // ZDNet (https://www.zdnet.com/article/ripe-discloses-failed-brute-force-attack-on-its-sso-service/). 18.02.2021).***

***

«По мнению аналитиков, невидимые пиксели, используемые для отслеживания активности электронной почты, теперь являются "повсеместной" проблемой, нарушающей нашу конфиденциальность.

На этой неделе служба обмена сообщениями Hey проанализировала свой трафик по запросу BBC и обнаружила, что примерно две трети электронных писем, отправленных на личные учетные записи электронной почты ее пользователей, содержат так называемые «шпионские пиксели».

Шпионские пиксели, также известные как пиксели отслеживания или веб-маяки, представляют собой невидимые крошечные файлы изображений, включая файлы.PNG и.GIF, которые вставляются в тело содержимого электронного письма.

Они могут быть прозрачными, белыми или другого цвета, сливаться с содержимым и оставаться невидимыми для получателя, и часто имеют размер всего 1 x 1 пиксель.

Получателю электронного письма не нужно напрямую взаимодействовать с пикселем, чтобы он мог отслеживать определенные действия. Вместо этого, когда открывается электронное письмо, автоматически загружается пиксель

отслеживания - и это позволяет серверу, принадлежащему маркетологу, знать, что письмо было прочитано. Серверы также могут записывать количество открытий электронной почты, IP-адрес, связанный с местоположением пользователя, и использование устройства.

Подобные пиксели также широко используются в веб-доменах для отслеживания посетителей.

Пиксели отслеживания существуют уже некоторое время, но о них мало что известно. Для маркетологов пиксели могут быть бесценным методом измерения уровней вовлеченности, оценки успеха маркетинговых кампаний и, возможно, для отправки последующих действий и более персонализированных заметок, когда сообщение было прочитано, но на него не ответили.

Однако, по словам соучредителя Ney Дэвида Хайнемейера Ханссона, они также представляют собой «гротескное вторжение в частную жизнь».

Ханссон сообщил изданию, что в среднем компания обрабатывает один миллион электронных писем и каждый день блокируется более 600 000 попыток отслеживания пикселей. Если вы доведете эти уровни до миллионов и миллионов электронных писем, обрабатываемых такими службами, как Gmail или Outlook, предположение о том, что использование пиксельного трекера является «эндемическим», может быть реалистичным.

В Европе GDPR требует, чтобы организации сообщали получателям об использовании таких пикселей. Тем не менее, вокруг прозрачности, необходимой для реализации отслеживания пикселей, была неясность, поскольку согласие не всегда требуется - и когда оно требуется, оно может быть `` получено '' автоматически, когда пользователь подписывается на службу электронной почты и его просят прочитать уведомление о конфиденциальности, опубликованное на веб-сайте.

Как отмечается в публикации, Управление комиссара по информации Великобритании (ICO), которое действует как сторожевой таймер защиты данных, использует пиксели для отслеживания открытий электронной почты в своем информационном бюллетене. Пользователи четко сообщают о трекерах при регистрации; однако ICO намеревается вскоре удалить эту функцию.

Можно предотвратить срабатывание пикселей отслеживания, запретив автоматическую загрузку изображений в вашем веб-браузере или загрузив надстройки электронной почты и браузера для блокировки трекеров». ***(Charlie Osborne. Tracker pixels in emails are now an 'endemic' privacy concern // ZDNet (https://www.zdnet.com/article/spy-pixels-in-emails-to-track-recipient-activity-are-now-an-endemic-privacy-concern/). 17.02.2021).***

***

«Singtel подтвердила, что личные данные 129 000 клиентов, а также финансовая информация его бывших сотрудников были скомпрометированы в результате взлома, связанного с использованием сторонней системы обмена файлами. Данные кредитной карты, принадлежащие персоналу корпоративного клиента, и информация, связанная с 23 предприятиями, в том числе поставщиками и партнерами, также просочились во время инцидента.

Объявление в среду было сделано менее чем через неделю после того, как сингапурская телекоммуникационная компания сообщила, что «файлы были захвачены» в результате атаки, затронувшей файловую систему под названием FTA, разработанную два десятилетия назад компанией Accellion. Singtel заявила, что использовала программное обеспечение для внутренних целей и с внешними заинтересованными сторонами.

После расследования компания сообщила, что скомпрометированные личные данные, принадлежащие 129 000 клиентов, содержали их идентификационный номер наряду с некоторыми другими данными, включая имя, дату рождения, номер мобильного телефона и физический адрес.

Также просочились данные банковских счетов 28 бывших сотрудников Singtel и данные кредитных карт 45 сотрудников корпоративного клиента с мобильными линиями Singtel. Кроме того, была скомпрометирована «некоторая информация» от 23 предприятий, включая поставщиков, партнеров и корпоративных клиентов.

Singtel не предоставила более подробной информации о том, что это за информация, ссылаясь на соображения безопасности.

Телефонная компания заявила, что большая часть утечки данных скомпрометировала внутреннюю информацию, которая не была конфиденциальной, например, журналы данных, тестовые данные, отчеты и сообщения электронной почты.

Он заявил, что начал уведомлять пострадавших лиц и предприятия о нарушении и предлагал помощь в снижении потенциальных рисков, связанных с нарушением. Это включало положения о том, что поставщик услуг передачи данных может предоставлять услуги мониторинга идентичности без дополнительных затрат затронутым клиентам, которые будут проинструктированы о том, как подписаться на услугу.

Генеральный директор группы Singtel Юэнь Куан Мун сказал: «Хотя эта кража данных была совершена неизвестными сторонами, мне очень жаль, что это произошло с нашими клиентами, и я безоговорочно извиняюсь перед всеми, кого это коснулось. Конфиденциальность данных имеет первостепенное значение. Мы разочаровали наших заинтересованных сторон и не встретились стандарты, которые мы для себя установили.

«Учитывая сложность и деликатность наших расследований, мы максимально прозрачны и предоставляем информацию, которая является точной, насколько нам известно», - сказал Yuen, добавив, что его расследование продолжается, чтобы установить полную степень нарушения.

Он отметил, что основные операции и функции Singtel не пострадали, и компания проводит «тщательную проверку» своих систем и процессов.

TELCO ТОЛЬКО НЕДАВНО СООБЩИЛА О ДАТЕ ОКОНЧАНИЯ ЖИЗНЕННОГО ЦИКЛА ПРОДУКТА.

На прошлой неделе ZDNet спросил Singtel, почему он все еще использует FTA, 20-летний продукт для обмена файлами, жизненный цикл которого, по словам Accellion, приближается к концу, но телефонная компания не ответила на этот вопрос.

В обновленном FAQ, размещенном на его веб-сайте, Singtel отметила, что продолжает использовать программное обеспечение, поскольку оно «все еще является текущим продуктом, предлагаемым и поддерживаемым Accellion». Компания сообщила, что Accellion объявила об окончании срока службы продукта только 28 января этого года, начиная с 30 апреля.

1 февраля Accellion опубликовал заявление, в котором говорилось, что его система FTA является устаревшей программой для передачи больших файлов, жизненный цикл которой приближается к концу.

Singtel сказал: «К сожалению, атака произошла, когда мы проводили обзор для обновления или замены продукта. И, несмотря на своевременное обновление исправлений уязвимостей, предоставленных Accellion, исправления не удалось».

На прошлой неделе телекоммуникационная компания сообщила, что первое исправление Accellion было развернуто 24 декабря, а второе исправление было применено 27 декабря. 23 января Accellion выпустил еще одно уведомление, ссылаясь на новую уязвимость, против которой исправление от 27 декабря оказалось неэффективным, согласно Singtel. Он сказал, что после того, как узнал об этом, он отключил систему FTA.

Последующий патч был предоставлен 30 января для устранения новой уязвимости, которая, по словам оператора, вызвала предупреждение об аномалии, когда были предприняты попытки ее развернуть. Компания Accellion уведомила его о том, что его система могла быть взломана 20 января, а после расследования Singtel 9 февраля подтвердила, что данные были скомпрометированы». ***(Eileen Yu. Singtel breach compromises data of customers, former employees // ZDNet (https://www.zdnet.com/article/singtel-breach-compromises-data-of-customers-former-employees/). 17.02.2021).***

***

«Австралийское право на данные о потребителях (CDR) официально запущено 1 июля с первым траншем, режимом открытого банковского обслуживания, требующим от поставщиков финансовых услуг предоставления данных о клиентах по запросу клиента.

Хотя первый транш CDR относится к отрасли финансовых услуг, вскоре к этому режиму присоединятся энергетика и телекоммуникации.

Данные могут быть переданы только аккредитованным получателям данных (ADR). Но уполномоченного по информации и конфиденциальности Австралии Ангелин Фальк беспокоит то, что «большие технологии» имеют возможность подать заявку на получение статуса ADR.

«В настоящее время крупные технологические компании и компании социальных сетей могут подать заявку на аккредитацию в качестве получателей данных в схеме CDR, однако я понимаю, что ни один из них в настоящее время не аккредитован, и мне не известны какие-либо конкретные варианты использования, почему они могут пожелать для вовлечения, поэтому в некотором смысле я говорю абстрактно», - сказала она.

Выступая перед Специальным комитетом Сената по финансовым технологиям и регуляторным технологиям в пятницу, Фальк сказал, что одной из

надежных защит в системе CDR является согласие потребителей и возможность отдельных лиц выбирать и контролировать то, как обрабатываются их данные.

Она обеспокоена тем, что это также может дать технологическим гигантам доступ к большему количеству данных, чем у них уже есть.

«Я думаю, что из-за обширных массивов данных, которые хранятся на некоторых платформах социальных сетей, необходимо будет позаботиться о том, чтобы люди понимали, на что они соглашаются, если их информация о правах потребителей будет объединена с этим [что] возможно, есть в их профиле в социальных сетях», - сказал Фальк.

«Некоторые из рисков, я думаю, связаны с выводами, которые можно извлечь из этой информации, и она может включать конфиденциальную информацию и использоваться способами, которых люди могут не ожидать».

Она задумалась, считает ли комитет, что цифровая платформа должна иметь доступ ко всем данным, или есть условие, что она не будет объединена с конфиденциальными данными, которые организация может уже иметь.

«Есть и другие проблемы, связанные с использованием алгоритмов и искусственного интеллекта при объединении данных, которые могут быть непрозрачными для потребителей и трудными для объяснения... [это] некоторые из проблем, связанных с получением полной информации и свободным предоставлением согласия, когда вы входите в очень сложные механизмы обработки данных», - добавила она.

Частные лица имеют возможность подать жалобу, если они считают, что их личная информация не обрабатывалась в соответствии с требованиями законодательства, и у OAIC было 20 «контактов» в отношении системы CDR.

«У нас есть роль сортировки, так что потребителям, которые участвуют в системе, не нужно ориентироваться в правительстве, чтобы подать жалобу или сделать запрос, поэтому они придут в наш офис, и мы отсортируем их по соответствующим», - пояснила заместитель комиссара Элизабет Хэмптон.

По ее словам, из этих 20 контактов у OAIC было две жалобы и восемь запросов в свой офис; и девять запросов и один «отчет», которые были отправлены в ACCC.

Хотя эти цифры невелики, Фальк сказал, что они отражают количество людей, задействованных в системе, ожидая, что это число будет расти вместе с внедрением схемы». ***(Asha Barbaschow. OAIC cautions giving big tech access to information under the Consumer Data Right // ZDNet (https://www.zdnet.com/article/oaic-cautions-giving-big-tech-access-to-information-under-the-consumer-data-right/). 12.02.2021).***

***

«Принятие Уолл-стрит утечки данных и «усталости» инвесторов заморозило реакцию трейдеров на инцидент с кибербезопасностью, как показывают новые исследования.

За последнее десятилетие стремление использовать данные для улучшения бизнес-операций, управления и взаимоотношений с клиентами не происходило одновременно с улучшением гигиены кибербезопасности для защиты этих данных

- и организации по-прежнему стремятся к огромным рискам для стоимости своих акций. день в результате.

Согласно последнему отчету IBM о стоимости утечки данных, корпоративный сектор может рассчитывать на средний счет в размере 3,86 миллиона долларов - но в случае крупных инцидентов безопасности, связанных с записями потребителей, он может вырасти до 392 миллионов долларов - за устранение нарушения.

Некоторые компании прячут голову в песок, когда им сообщают об утечке данных, будь то открытая корзина, вторжение, инсайдерские операции или случайная потеря информации.

Однако для предприятий, торгующих на публичных платформах фондового рынка, неспособность распознать утечку данных или попытки ее скрыть могут иметь реальные долгосрочные последствия.

На этой неделе Comparitech опубликовала свой годовой отчет о том, как утечки данных могут повлиять на цены акций, который показал, что инциденты, связанные с кибербезопасностью, не имеют таких же разветвлений для фондового рынка, как почти десять лет назад.

В этом году исследование выявило 34 компании и 40 публично раскрытых утечек данных. Компании были выбраны на основании утечки данных, включающей не менее одного миллиона записей, последующего публичного раскрытия информации и активного листинга на NYSE.

Есть некоторые ограничения исследования, включая возможные размеры выборки на основе критериев Comparitech, а также влияние финансовых отчетов и проблему коллективных исков.

«Если утечка данных приводит к утечке особенно опасной информации, которая в конечном итоге приводит к финансовому ущербу для клиентов компании, и было доказано, что компания не обеспечила надлежащую защиту информации, просочившейся в результате этой утечки, клиенты часто подают в суд [..]», - отмечают исследователи. "Обычно это приводит к расчетам, в которых компания выкладывает миллионы долларов, чтобы возместить клиентам ущерб. Это не всегда происходит, и выплачиваемые суммы варьируются, поэтому у нас просто не хватает данных, чтобы соответствовать практической модели, которая показывает как эти расчеты влияют на цены акций».

Однако исследование все же выявляет некоторые интересные тенденции. Цена акций взломанной компании теперь падает в среднем на 3,5% в течение 14 дней с момента раскрытия информации и достигнет минимальной отметки примерно через 110 рыночных дней. Предварительный анализ проведен в 2019 году предположил, что цены на акции будут падать в среднем на 7,27%.

Низкая доходность Nasdaq в среднем находится в диапазоне -3,5%, и 21 из 40 нарушений привели к ухудшению показателей акций в течение шести месяцев после нарушения по сравнению с шестью месяцами ранее. В среднем цены на акции выросли на 2,6% до нарушения и упали на 3% после этого.

Одна примечательная тенденция состоит в том, что «старые нарушения» когда-то были встречены Уолл-стрит более немедленной и негативной реакцией. Цены на акции упали более существенно, и, согласно исследованию, на

восстановление акций требовалось в среднем 109 дней, когда в 2012 году и ранее произошла утечка.

Для утечек данных, произошедших в период с 2013 по 2016 годы, падение цены акций было «менее серьезным», чем в более ранней категории, и разница в стоимости между шестью месяцами до и после раскрытия инцидента безопасности составляла менее 1%.

Что касается нарушений, о которых сообщалось в 2017 году и позже, для восстановления цен потребовалось примерно 100 дней, а общие показатели были лишь «немного хуже» в течение шести месяцев после нарушения.

Согласно Comparitech, на сегодняшнем рынке больше всего пострадали от утечки данных компании, оказывающие технологические и финансовые услуги, тогда как компании электронной коммерции и социальных сетей пострадали «меньше всего».

«Нарушения, которые приводят к утечке очень конфиденциальной информации, такой как номера кредитных карт и социального страхования, в среднем приводят к более быстрому падению цен на акции, чем компании, которые утекают менее конфиденциальную информацию, но в долгосрочной перспективе они не обязательно пострадают больше», - отметили исследователи.

Влияние утечки данных на цены акций компании, похоже, со временем уменьшается по мере того, как память исчезает, и есть много других факторов, которые также могут отрицательно повлиять на стоимость акций организации, например, сбой, вызванный COVID-19, несвязанные судебные процессы и руководство. изменения». ***(Charlie Osborne. Investor data breach 'fatigue' reduces Wall Street punishment for cybersecurity failures // ZDNet (https://www.zdnet.com/article/investor-data-breach-fatigue-reduces-wall-street-punishment-for-cybersecurity-failures/). 10.02.2021).***

***

«Гигант супермаркетов Kroger пострадал от утечки данных после того, как служба, используемая для безопасной передачи файлов, была взломана, а злоумышленники украли файлы.

Kroger - один из крупнейших розничных торговцев в мире с почти 2800 магазинами в 35 штатах. В Kroger работает около 500000 человек, а объем продаж в 2019 году составил более 122 миллиардов долларов.

Вчера Крогер сообщил, что они были последней компанией, пострадавшей от уязвимости в программном обеспечении Accellion FTA, которая позволяла хакерам красть данные у компаний, использующих эту услугу.

Согласно сообщению об утечке данных, опубликованному вчера, Крогер был проинформирован Accellion об их нарушении 23 января 2021 года и немедленно прекратил использование сервиса.

В рамках расследования атаки Крогер установил, что нарушение не повлияло на данные продуктового магазина, включая информацию о платежах. Однако в результате взлома были обнаружены данные о людских ресурсах и аптеки.

«В настоящее время, основываясь на информации, предоставленной Accellion, и на нашем собственном расследовании, Крогер полагает, что категории

затронутых данных могут включать данные по персоналу определенных партнеров, определенные записи аптек и определенные записи денежных услуг».

«Важно отметить, что это не повлияло на данные или системы продуктового магазина; информацию о кредитных или дебетовых картах; или пароли учетных записей клиентов», - пояснил Крогер в своем сообщении об утечке данных.

Крогер заявляет, что они связываются с пострадавшими по почте. Для пострадавших Kroger предлагает год бесплатного кредитного мониторинга.

Атаки Accellion имеют широкое влияние

Kroger - лишь одна из тех, что пополняется длинным списком компаний, пострадавших от уязвимости в сервисе Accellion FTA, которую хакеры использовали в последние несколько месяцев.

В середине декабря Accellion сообщила, что они узнали об активно эксплуатируемой уязвимости нулевого дня в их службе безопасной передачи файлов FTA. Злоумышленники использовали эту уязвимость для кражи данных у компаний, которые использовали сервис для безопасного взаимодействия с клиентами и партнерами.

Accellion выпустил патч на Рождество, но к тому времени, когда компании получили обновление и применили его, злоумышленники уже получили доступ к своим данным.

Некоторые из тех, кто пострадал от взлома Accellion, получили записки с требованием выкупа от злоумышленников, в противном случае их данные будут опубликованы.

Поскольку сервис Accellion FTA используется многими компаниями, образовательными учреждениями и государственными учреждениями, мы продолжим получать сообщения о взломе данных со временем.

Предыдущие нарушения данных, связанные с Accellion, включают Singtel, QIMR Berghofer Medical Research Institute, Резервный банк Новой Зеландии, Австралийскую комиссию по ценным бумагам и инвестициям (ASIC) и Управление аудитора штата Вашингтон («SAO»)». ***(Lawrence Abrams. Kroger data breach exposes pharmacy and employee data // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/kroger-data-breach-exposes-pharmacy-and-employee-data/). 20.02.2021).***

***

Нарушение данных Singtel

Singtel, крупнейший оператор мобильной связи в Сингапуре, объявил сегодня о взломе данных, вызванном уязвимостью службы Accellion FTA.

«Сторонняя система обмена файлами, предоставляемая Accellion под названием FTA, была подвергнута незаконному доступу через уязвимость нулевого дня или ранее неизвестную уязвимость. Singtel использует эту систему для обмена информацией внутри компании, а также с внешними заинтересованными сторонами и организациями», - заявила Singtel в своем заявлении. уведомление об инциденте безопасности.

Телекоммуникационная компания не раскрывает, к каким данным был получен доступ в ходе атаки, и заявляет, что в настоящее время выясняет, кто пострадал.

"Учитывая сложность расследований, потребуется время, чтобы провести оценку воздействия. Мы работаем в срочном порядке, чтобы определить характер и объем данных, к которым потенциально был доступ. Мы свяжемся с отдельными лицами и организациями, информация которых может были скачаны незаконно», - продолжил Сингтел.

В то время как расследование продолжается, Singtel заявляет, что они отключили систему FTA, пока проводят расследование нарушения.

Как только будет определено, к чему получили доступ злоумышленники, они начнут связываться с затронутыми людьми.

QIMR Berghofer также пострадал

Медицинский исследовательский институт QIMR Berghofer также объявил сегодня об утечке данных, вызванной службой Accellion FTA, и предоставил более подробную информацию о том, к какой информации был получен доступ.

По данным исследовательского института, утечка данных произошла 25 декабря 2020 года, когда злоумышленники получили доступ примерно к 4 процентам, или 620 МБ, данных, хранящихся в сервисе Accellion FTA.

QIMR Berghofer заявляет, что они получили свое первое уведомление об установке патча Accellion 4 января 2021 года. Только 2 февраля 2021 года Accellion уведомил их о том, что у них произошла утечка данных.

«Первое уведомление QIMR Berghofer получило от Accellion 4 января 2021 года, когда компания посоветовала Институту применить исправление безопасности. Институт немедленно отключил программное обеспечение и применил исправление».

«Accellion уведомил QIMR Berghofer во вторник, 2 февраля 2021 года, что, по его мнению, Институт пострадал от утечки данных, которая также затронула ряд других австралийских и международных клиентов Accellion», - сообщил QIMR Berghofer в уведомлении об утечке данных на своем веб-сайте.

Исследовательский институт заявляет, что они используют службу FTA для получения и отправки данных о клинических испытаниях противомалярийных препаратов, а также для обмена данными с Комитетом по исследованиям комаров и арбовирусов.

Однако перед сохранением в Accellion общие данные анонимизируются, и участникам испытаний присваиваются коды для их идентификации.

«Обезличенная» информация, хранящаяся ими на Accellion, включает инициалы, дату рождения, возраст, пол и этническую группу участников клинических испытаний, а также коды участников. Некоторые документы также содержат анамнез неидентифицированного характера.

QIMR Berghofer также заявляет, что резюме примерно для 30 сотрудников службы Accellion FTA.

Отсутствие идентифицирующей информации в данных, хранящихся на устройстве FTA, - палка о двух концах.

Хотя никакая личная информация не была раскрыта, поскольку каждый участник испытания был деидентифицирован и ему были присвоены коды для обозначения его, QIMR Berghofer не имеет возможности связаться с ними.

«Мы не можем связаться с этими участниками клинических испытаний, потому что мы не знаем, кто они, и не знаем их имен или контактных данных. Тем не менее, если у кого-то есть какие-либо проблемы или ему нужна дополнительная информация, он может связаться с нами, используя указанные ниже данные.

«Мы связываемся с нашими партнерами по клиническим испытаниям и другими заинтересованными сторонами, чтобы сообщить им, что произошло и что мы делаем для устранения этой вероятной утечки данных», - поясняет QIMR Berghofer». ***(Lawrence Abrams. Singtel, QIMR Berghofer report Accellion-related data breaches // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/singtel-qimr-berghofer-report-accellion-related-data-breaches/). 11.02.2021).***

***

«Профессиональное веб-сообщество SitePoint обнаружило утечку данных после того, как их пользовательская база данных была продана и в конечном итоге бесплатно просочилась на хакерский форум.

SitePoint - это веб-сайт, запущенный в 1999 году, который предлагает контент и сообщество, посвященное веб-профессионалам и разработчикам. Сайт предлагает премиум-членство, которое обеспечивает доступ к более чем 600 книгам, курсам и выступлениям.

В конце декабря 2020 года BleepingComputer узнала о брокере по утечке данных.

Одна из баз данных была для SitePoint.com, который, по заявлению брокера, содержал миллион пользовательских записей.

В то время BleepingComputer связался с SitePoint с этой информацией, но мы так и не получили ответа на наши повторяющиеся электронные письма.

26 января 2021 года злоумышленник, известный как ShinyHunters, бесплатно поделился базой данных Learnable.com на хакерском форуме. Learnable.com перенаправляет на домен Sitepoint.com.

Эта база данных содержит 1 020 959 человек, включая имена участников, адреса электронной почты, хешированные пароли bcrypt, дату рождения, страну, IP-адрес, использованный при регистрации, и другую информацию.

SitePoint раскрывает утечку данных

На этой неделе пользователи SitePoint сообщили BleepingComputer, что они получали электронные письма с вымогательством и поддельными раздачей криптовалюты на адреса, которые, по их утверждению, были специально созданы и использовались только в SitePoint.

После того, как эти пользователи пожаловались SitePoint, компания раскрыла утечку данных, подтвердив, что злоумышленники взломали их системы и украли данные участников.

«Недавно мы подтвердили, что инфраструктура SitePoint была взломана третьей стороной, и в ходе этой атаки был получен доступ к неконфиденциальным данным клиентов».

«В качестве меры предосторожности, пока мы продолжаем расследование, мы сбросили пароли для всех учетных записей и увеличили требуемую длину до 10 символов. В следующий раз, когда вы войдете в SitePoint, вам нужно будет создать новый пароль», - заявляет SitePoint в утечке данных. уведомление отправлено BleepingComputer.

SitePoint сообщает, что хакеры получили доступ с помощью скомпрометированного стороннего инструмента, используемого для мониторинга их учетной записи GitHub. SitePoint считает, что с помощью этого инструмента и украденных ключей API злоумышленники могут получить доступ к их кодовой базе и системе.

Хотя SitePoint не раскрывает имя скомпрометированного стороннего инструмента, оно соответствует описанию взлома приложения Waydev, которое хакеры использовали для взлома других сайтов за последний год.

SitePoint заявляет, что они сбросили пароли для всех учетных записей, но те учетные записи, которые настроены на автоматический вход, все равно будут делать это. Для этих пользователей SitePoint рекомендует пользователям вручную изменить свой пароль через «Учетная запись> Профиль и настройки».

Никакая финансовая информация, такая как кредитные карты, не хранится в их системе, и злоумышленник не получил доступа к ней…». ***(Lawrence Abrams. SitePoint discloses data breach after stolen info used in attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/sitepoint-discloses-data-breach-after-stolen-info-used-in-attacks/). 05.02.2021).***

***

«…Заместители послов ЕС в среду подписали Регламент электронной конфиденциальности, который направлен на защиту конфиденциальности онлайн-коммуникаций путем регулирования того, как операторы связи, технологические компании и индустрия онлайн-рекламы используют личные данные.

Несмотря на долгий путь к принятию закона - окончательный вариант законопроекта должен быть согласован между представителями Совета ЕС, Европейской комиссии и Европейского парламента - одобрение на этой неделе является большим шагом вперед после многих лет споров между национальными столицами без большой прогресс.

«Путь к позиции в Совете был нелегким, но теперь у нас есть мандат, который обеспечивает хороший баланс между надежной защитой частной жизни людей и содействием развитию новых технологий и инноваций», - сказал министр инфраструктуры Португалии Педро Нуно Сантос., который провел встречу в среду, потому что Португалия в настоящее время председательствует в Совете.

Текст был впервые представлен Комиссией в январе 2017 года, через несколько месяцев после того, как была завершена флагманская реформа защиты данных в Европе - Общий регламент по защите данных (GDPR).

Правила электронной конфиденциальности были одобрены парламентом, который принял свою версию в октябре 2017 года, и защитниками цифровых прав, но сразу же подняли тревогу в европейских столицах и в промышленности.

До среды восемь стран, возглавляющих Совет ЕС, пытались, но безуспешно, найти соглашение между правительствами. Не помогло и то, что законопроект стал объектом одной из самых интенсивных кампаний по влиянию, когда-либо существовавших в отношении цифровых файлов. Big Tech, европейские операторы связи и издатели прессы интенсивно лоббировали этот текст, утверждая, что он будет препятствовать инновациям и ограничить плюрализм СМИ.

По словам дипломатов ЕС, которые работали над переговорами, законопроект повлиял на очень много разных вещей, включая онлайн-рекламу, СМИ, телекоммуникации и национальную безопасность, что было трудно найти компромисс, который работал бы для большинства столиц.

Каждый раз, когда председательство в ЕС пыталось угодить некоторым недовольным столицам, изменяя текст, они теряли поддержку других, которые чувствовали, что баланс нарушен.

«Это немного проклятый текст», - сказал один чиновник ЕС.

Длительные переговоры высветили сложность поиска компромисса между защитой данных и инновациями, а также то, как многие компании, которые начали согласованную борьбу, чтобы убить или хотя бы ослабить закон, полагаются на сбор личных данных. Поскольку изнурительные переговоры по доработке GDPR еще не закончились, Совет в какой-то момент выдохся.

Весной 2018 года стало очевидно, что в таких могущественных столицах, как Париж, нет готовности завершить переговоры до окончания срока Жан-Клода Юнкера на посту президента Комиссии, несмотря на то, что до конца осталось полтора года. В ноябре того же года, все надежды были мертвы достижения соглашения о файле перед новым парламентом и Комиссией будет взять на себя.

Регламент электронной конфиденциальности также является хрестоматийным примером того, как сложно принять законодательство, когда Франция и Германия, два тяжеловеса ЕС, не синхронизированы. Подход Берлина, ориентированный на конфиденциальность, разошелся с Парижем, который хотел более мягких правил для издателей прессы и операторов связи, а также полномочий надзора для себя, чтобы помочь своей борьбе с преступностью и терроризмом.

При последнем голосовании на этой неделе Париж поддержал текст после некоторых изменений в последнюю минуту, а Берлин воздержался.

Это история переговоров, основанная на беседах и интервью с десятками официальных лиц ЕС, промышленными лоббистами, активистами и политиками за четыре года напряженных переговоров. Многие говорили с POLITICO на условиях анонимности, чтобы обсудить конфиденциальные переговоры более откровенно.

С 2017 года законопроект пережил восемь президентств ЕС и две комиссии и парламента до голосования в среду под председательством Португалии.

Регламент электронной конфиденциальности уже находился в режиме жизнеобеспечения, когда он впервые поступил в Совет.

Еще до того, как Комиссия официально представила его, промышленность лоббировала отказ от своей предшественницы - Директивы об электронной конфиденциальности. Операторы связи хотели более свободно использовать метаданные местоположения; издатели хотели продолжать использовать файлы cookie в целях целевой рекламы; Big Tech опасались своей бизнес-модели, основанной на личных данных.

Между тем в Совете, потратив годы на переговоры о правилах конфиденциальности для GDPR, столицы стран, включая Варшаву и Дублин, заявили, что не понимают, как новые правила Комиссии будут работать вместе с законом, который они только что приняли. Это стало бы одним из главных аргументов в Совете, чтобы задержать принятие закона.

«Первые годы работы над реформой в Совете были посвящены демонстрации необходимости этого регулирования, - сказала Эстель Массе, старший политический аналитик НПО «Доступ сейчас» в области цифровых прав. «В течение нескольких лет отсутствовала политическая воля для продвижения эта реформа».

Задача усложнялась еще и тем, что некоторые правительства не могли определиться с позицией, заявили несколько дипломатов ЕС.

В Берлине министерства экономики и юстиции спорили из-за этого предложения - даже когда сама Германия пыталась заключить соглашение во время своего председательства в ЕС в прошлом году. Министерство экономики хотело более мягких правил, которые, по его мнению, будут способствовать инновациям и развитию искусственного интеллекта; Минюст настаивал на высоком уровне защиты данных. (Справедливость победила: президентство Германии сняло пункт, позволяющий обрабатывать метаданные «дальше».)

Лоббистская суета

Совет также зашел в тупик из-за ошеломляющего лоббирования закона в отрасли.

В течение многих лет отраслевые группы, такие как технологическое лобби DigitalEurope, телекоммуникационные лобби ETNO и GSMA, лобби публикаций прессы EMMA / ENPA (включая Акселя Спрингера, совладельца POLITICO Europe) и многие, многие другие отправляли бесчисленное количество писем как в Брюссель, так и в национальные правительства. попытаться повлиять на политиков. Операторы связи и технологические компании пытались добиться полной отмены законодательства.

«Одна из худших лоббистских кампаний, которые я когда-либо видел», - так описал ее один парламентский инсайдер, цитируемый в отчете Корпоративной европейской обсерватории за 2018 год, неправительственной организации по вопросам прозрачности.

Европейские компании успешно использовали тактику, чтобы доказать, что это предложение может еще больше укрепить американских технологических гигантов.

Исходный текст Комиссии позволял пользователям устанавливать настройки конфиденциальности в своих интернет-браузерах. Но с преобладанием браузеров, принадлежащих Google, Apple и Microsoft, европейские отрасли утверждали, что

текст предоставил бы американским компаниям больший контроль над онлайн-опытом европейских пользователей.

В результате правительства ЕС исключили из текста положения о настройках конфиденциальности, несмотря на протесты защитников цифровых прав.

Другая тактика заключалась в том, чтобы разделять и властвовать.

Согласно документу от 2017 года, с которым ознакомился POLITICO, гигант электронной коммерции Amazon хвастался тем, что ослабил поддержку этого предложения европейскими законодателями. Разделив депутатов Европарламента, Amazon надеется, что «ослабит позицию парламента на переговорах с Советом, который более благосклонен к озабоченности отрасли», говорится в документе.

«Наша кампания гарантирует, что предложение об электронной конфиденциальности не получит широкой поддержки в Европейском парламенте», - говорится в документе.

Корпоративная европейская обсерватория отметила значительный интерес к правилам со стороны таких различных секторов, как интернет-магазины модной одежды, сайты бронирования отелей и производители игрушек, помимо рекламной индустрии и крупных технологий.

Дальнейшие осложнения

Попутно новые вопросы еще больше осложнили переговоры в Совете.

С 2018 года столицы, включая Лондон и Дублин, подстрекаемые технологической индустрией, в том числе Facebook, утверждали, что правила конфиденциальности будут препятствовать борьбе с сексуальным насилием над детьми в Интернете, что еще больше отодвинуло обсуждение Совета, заявили два представителя ЕС.

Комиссия заявила, что это не так, но в конечном итоге в сентябре прошлого года пришлось пойти на отступление от правил, чтобы позволить технологическим компаниям обнаруживать и удалять материалы о сексуальном насилии над детьми без согласия.

Комиссия разработала отступление отчасти для того, чтобы устранить то, что стало одной из самых острых проблем Регламента электронной конфиденциальности, и открыть путь к одобрению законопроекта, сказал представитель Комиссии.

«Интернет-материалы о сексуальном насилии над детьми были одной из самых сложных проблем во время президентства Финляндии», - сказал один из официальных лиц ЕС. «[Предложение Комиссии] решило эту проблему и стерло ее со стола».

Вопрос о том, как долго компании должны хранить информацию о гражданах для доступа правительства и полиции, известный как хранение данных, оставался камнем преткновения до самого конца.

В феврале 2019 года заинтересованные в безопасности государства, включая Бельгию, Эстонию, Данию, Францию и Великобританию, написали необязательный документ, в котором утверждали, что Регламент электронной конфиденциальности должен допускать «возможность для существующих и будущих режимов хранения данных». Они утверждали, что положение о хранении

данных необходимо для «предотвращения, расследования, обнаружения или преследования уголовных преступлений».

Когда в октябре прошлого года Суд ЕС постановил, что схемы хранения данных во Франции и Бельгии не соответствуют действующему законодательству ЕС, это усилило давление на переговоры об электронной конфиденциальности.

В среду Франция воздержалась от поддержки текста до тех пор, пока португальское президентство не внесет в последний момент некоторые изменения, которые откроют двери для стран ЕС, чтобы сохранить данные. Окончательное предложение Совета отражает пожелания Парижа, согласно внутренней записке французских властей, полученной НПО по цифровым правам Access Now через запрос доступа к документу и переданной POLITICO.

Финский компромисс

В конце прошлого года стало ясно, что единственный способ получить большинство - это вернуться к тексту, предложенному финским председательством осенью 2019 года.

Хельсинки также не смог прийти к соглашению - хотя он стал ближе, чем кто-либо другой.

В ноябре 2019 года Финляндия надеялась, что ее компромиссный текст получит достаточную поддержку, но более дюжины стран, включая Францию и Германию, отклонили это предложение - некоторые из-за того, что считали, что текст поставит компании в тупик, другие из-за опасений, что конфиденциальность не будет нарушена. быть достаточно защищенным.

Но были и другие факторы, как пояснил один из официальных представителей ЕС, участвовавший в переговорах. Делегации ЕС все еще надеялись, что недавно созданная Комиссия фон дер Ляйена внесет новое предложение, и они ждали, пока Суд ЕС вынесет решение по делу о сохранении данных. Дискуссии о сексуальном насилии над детьми в Интернете - до того, как Комиссия придумала отступление - также усложнили ситуацию.

И «очень большой лоббистский толчок» индустрии побудил столицы отклонить текст, добавил чиновник.

Хорватия, принявшая председательство в январе 2020 года, решила сделать текст более дружественным к отрасли. В результате недолгой победы для издательской, технической и телекоммуникационной отраслей Загреб выдвинул новые предложения, которые позволили бы компаниям обрабатывать метаданные и собирать информацию с электронных устройств пользователей без их согласия, «если это необходимо для целей законной интерес." Это положение не понравилось Совету.

Германия, которая приняла председательство в Совете в июле 2020 года, пошла в противоположном направлении и представила текст, более дружественный к конфиденциальности. Берлин удалил пункт о законных интересах Хорватии, а также исключил положение, которое позволяло компаниям обрабатывать метаданные пользователей без их согласия, если цель совместима с тем, на что пользователи изначально соглашались. Но и это не понравилось Совету.

«Так оказалось, что финский компромисс был лучшим», - сказал представитель ЕС.

Предложение португальского председательства эффективно перекомпоновало финский компромисс с дополнительными поправками, которые, по их мнению, были необходимы для утверждения законопроекта.

Несмотря на то, что неправительственные организации, занимающиеся цифровыми правами, и ведущий переговорщик Европейского парламента считают, что текст Совета недостаточно защищает конфиденциальность, несмотря на то, что их называют промежуточными. Настройки конфиденциальности в браузерах по-прежнему отсутствуют, компании по-прежнему могут отказывать в доступе к своим веб-сайтам пользователям, которые не принимают файлы cookie, а положение об обработке метаданных, отброшенное немцами, вернулось в текст.

«Очевидно, что позиция парламента по-прежнему заключается в том, что мы должны защищать частную жизнь и конфиденциальность сообщений. Судя по тому, что мы слышим от Совета, я не уверен, что их позиция пойдет в этом направлении», - заявила депутат Европарламента Биргит Сиппель ранее на этой неделе, перед выступлением в среду. соглашение.

Федеральный регулятор защиты данных Германии заявил, что законопроект Совета является «серьезным ударом по защите данных».

Принятие законопроекта знаменует лишь конец начала для текста, который теперь станет предметом дополнительных переговоров, лоббирования и поворотов сюжета, поскольку европейские законодатели и национальные столицы готовятся к заключительным переговорам, которые могут продлиться до следующего года.

"Я не могу сказать вам, сможем ли мы получить окончательный текст уже в течение этого года, потому что нам нужно более подробно изучить детали, чтобы выяснить, где при всех различных позициях мы, тем не менее, можем найти общее понимание - переговоры будут непростыми, "Сказал Сиппель.

«Но всегда есть шанс на компромисс». ***(LAURA KAYALI, VINCENT MANANCOURT. How Europe's new privacy rules survived years of negotiations, lobbying and drama // POLITICO (https://www.politico.eu/article/europe-privacy-rules-survived-years-of-negotiations-lobbying/). 10.02.2021).***

***

«Кибератаки учащаются, усиливая угрозы конфиденциальности данных, которые они представляют как для государственных учреждений, так и для предприятий. Правительствам как внутри страны, так и за рубежом необходимо активизировать усилия по принятию в этом году закона, который укрепляет технологическую защиту, предупреждают группы по вопросам конфиденциальности.

Более жесткие законы о конфиденциальности постепенно пересматриваются и принимаются на рынке США. Но в основном этот процесс происходит на государственном уровне.

Между тем кибератаки представляют для ИТ-экспертов и законодателей войну на два фронта. Индустрия программного обеспечения борется с проблемами безопасности, которые делают кибератаки жизнеспособными. Государственные чиновники и руководители предприятий борются со сложными юридическими

вопросами, связанными с устаревшими или отсутствующими средствами защиты конфиденциальности.

Более крупные и успешные вторжения в правительство, бизнес и персональные компьютеры - обычное дело. Фишинговые кампании и атаки программ-вымогателей регулярно находят новых жертв. Ситуация очень похожа на игру Whack-a-Mole.

Защитники конфиденциальности видят больше возможностей для вступления в силу законов о конфиденциальности, поскольку они сосредоточены на том, чтобы подтолкнуть федеральных законодателей к принятию более строгих законов о конфиденциальности потребителей в ближайшие годы. Эти новые законы должны уделять первоочередное внимание новым технологиям, таким как искусственный интеллект (AI), машинное обучение (ML), облачные вычисления и блокчейн.

«Я ожидаю усиления регулирования, особенно когда речь идет о законах штатов, касающихся конфиденциальных персональных данных», - говорит Скотт Пинк, специальный советник в офисе международной юридической фирмы O'Melveny & Myers в Кремниевой долине и член отдела безопасности данных фирмы. и Privacy Group.

Pink регулярно консультирует СМИ и технологические компании о том, как соблюдать текущие государственные и отраслевые правила конфиденциальности. Он считает, что 2021 год может ознаменовать новую эру в законах о конфиденциальности, направленных на защиту широкого спектра ценной цифровой информации.

«Данные о состоянии здоровья COVID-19 вызывают непосредственную озабоченность по мере того, как мы переходим к следующей фазе пандемии. Правительства и системы здравоохранения собирают огромные объемы отслеживаемых контактов и информации, связанной с вакцинами. Внедрение законов, политик и процедур для обеспечения целостности этих данных данные будут иметь ключевое значение», - сказал Пинк TechNewsWorld.

Он подчеркнул, что кибератаки представляют собой значительный риск, особенно с учетом того, что удаленная работа и растущая изощренность фишинга и атак социальной инженерии создают больше уязвимостей, чем когда-либо прежде. Кибератаки и их влияние на конфиденциальность данных могут серьезно повлиять на деятельность государственных учреждений, компаний, школ и других организаций.

Крысы в атакующем миксе

Самыми распространенными угрозами, скрывающимися в 2021 году, являются заражения RAT. Аббревиатура RAT означает «троян для удаленного доступа» - разновидность вредоносного ПО, которое позволяет хакерам удаленно управлять устройствами.

Как только программа RAT подключена к компьютеру, хакер может просматривать локальные файлы, получать учетные данные для входа и другую личную информацию или использовать соединение для загрузки вирусов, которые затем могут без ведома пользователя распространяться среди других.

«Вторжение удаленного доступа может быть проблематичным, особенно с учетом того, что миллионы людей сейчас работают из дома», - отметил Роберт Сицилиано, инструктор по киберсоциальной защите личности в ProtectNow.

«Протокол удаленного рабочего стола Microsoft и многочисленные сторонние технологические сервисы удаленного доступа значительно увеличивают поверхность атаки для хакеров, желающих проникнуть в корпоративные и правительственные сети», - сказал он TechNewsWorld.

Он отметил, что некоторые из кибератак основаны на усиленной тактике, доступной после пандемии, и отличаются от таковых до прошлого года. Ни корпоративная Америка, ни местные, государственные и федеральные правительства никогда не ожидали этого.

Фактор облачности тоже имеет значение

Тем не менее, хакеры не добиваются успеха только с помощью современных высокотехнологичных тактик. По словам Наамы Бен Дов, сотрудника YL Ventures, американо-израильской фирмы венчурного капитала, сегодняшние угрозы представляют собой эскалацию существующих методов угроз, которые существуют уже много лет и которые были ускорены за счет еще более широкого использования облачных вычислений и гибкой разработки. которая специализируется на инвестициях в кибербезопасность на начальном этапе.

Миграция в облако - это большая часть проблем с конфиденциальностью данных, которые мы наблюдаем сегодня. Данные остаются главной целью для злоумышленников. Таким образом, кража данных является самой распространенной угрозой в этом году, настаивает Эльдад Чай, соучредитель и генеральный директор Satori Cyber, фирмы по доступу к данным и управлению в Тель-Авиве, которая входит в портфель YL Ventures.

«Посредством доступа к данным корпорации злоумышленники могут нанести репутационный, правовой и производственный ущерб, несоразмерный любому другому вектору атаки», - сказал он TechNewsWorld.

Конечно, большая часть этих данных находится в облаке. Тенденция перемещения данных в облако за последние годы усилилась и сейчас достигла рекордного уровня благодаря успеху таких платформ, как Snowflake, и ускорению 2020, предоставленному программам миграции в облако, отметил Чай.

«Массовая миграция данных в облако, демократизация данных внутри организации и среда работы из дома расширили поверхность для атак на данные и чрезвычайно затруднили выполнение эффективной программы защиты данных», - сказал Чай.

WFH также проблематичен

Сценарий «работа на дому» значительно упростил работу хакеру. Злоумышленники следят за своими целями, заметил Бен Дов. Сейчас, более чем когда-либо, эти данные перемещаются между компьютерами домашних работников, рабочими местами в офисе и банками облачных хранилищ.

Принято считать, что в офисе работники более продуктивны; По словам Сицилиано, когда разразился COVID, ИТ-менеджеры были по большей части неподготовленными.

Хотя некоторые компании развернули техническую помощь своим сотрудникам, использующим свои собственные компьютеры и маршрутизаторы дома, для обеспечения безопасности устройств вне сети, этого было недостаточно.

«Работать дома с устройствами, подключенными к корпоративным сетям с неправильной конфигурацией, - это самый большой страх ИТ-менеджера», - сказал он.

Слишком маленький, слишком поздно

В США существующие федеральные законы, такие как Закон о расширении удаленной работы от 2010 года, никогда не предусматривали, например, такого уровня работы дома. По мнению Сицилиано, федеральное правительство вряд ли в ближайшее время внесет какие-либо существенные изменения из-за множества других опасных для жизни проблем.

Одна из растущих угроз нарушениям конфиденциальности данных - программы-вымогатели. Но это следствие, а не причина потери конфиденциальности. Он отметил, что в конечном итоге программы-вымогатели становятся результатом работы трояна или технологии удаленного доступа.

«ИТ-менеджеры должны проявлять большую активность, предлагая оборудование, конфигурации программного обеспечения и обучение безопасности, - сказал Сицилиано о предотвращении разглашения конфиденциальности данных.

Новые технологии угрожают эффективности

По словам Бена Дова из YL Ventures, среди наиболее распространенных угроз конфиденциальности, с которыми мы столкнулись в 2021 году, стала зависимость от сторонних ИТ-сервисов, которые все чаще вытесняют или заменяют приложения, которые исторически развертывались локально.

«Как и в случае с SolarWinds, многие атаки на цепочки поставок нацелены на системы управления ИТ, которые использовались задолго до появления облака. Организации по-прежнему зависят от этой тактики, и эта атака заставит переосмыслить степень воздействия ИТ на цепочку поставок, "сказала она TechNewsWorld.

То же самое относится и к программным приложениям, продолжила она. В последние годы наблюдается стремительный рост количества стороннего программного обеспечения. Эта реальность заставляет организации терять видимость рисков, связанных с воздействием указанных сторонних компонентов.

Бен Дов предупредил, что эта ситуация, несомненно, ухудшится, прежде чем станет лучше. Все больше и больше увеличивается количество нарушений конфиденциальности данных, особенно личных данных.

«До тех пор, пока отсутствуют значимые технологические подходы к идентификации и защите данных, неизбежно произойдет множество утечек», - сказала она.

Исправить то, что сломано

Многие существующие решения ориентированы на управление данными и соблюдение нормативных требований. Эти цели важны, но не нацелены на корень проблемы. По словам Бен Дов, они хороши только в той мере, в какой действуют определенные правила.

«Нам нужны решения, которые способны отслеживать и контролировать данные на протяжении всего жизненного цикла таким образом, чтобы они были значимо интегрированы с существующими бизнес-подразделениями организаций и позволяли им выполнять, а не сдерживать НИОКР, продажи и маркетинг. Безопасность должна быть перекрестной - интерес предприятия и цель, которая поддерживает бизнес-процессы», - возразила она.

В настоящее время законодатель в основном сосредоточен на наших правах личности на неприкосновенность частной жизни. Хотя это приветствуется и необходимо, при этом не учитывается реализация программ конфиденциальности, и каждая компания имеет свой собственный способ соблюдения требований конфиденциальности, предлагаемых Satori Cyber's Chai.

«Сосредоточение законов на результатах, например, если данные потеряны, вас оштрафуют, не решает многие из основных проблем, связанных с фактической защитой частной жизни людей», - сказал он.

Чай не уверен, что это произойдет в этом году. Но он надеется, что правительства будут лучше справляться с определением и стандартизацией программ защиты данных таким образом, чтобы они помогли отрасли в реализации эффективных и устойчивых программ.

Новая конфиденциальность, проблемы с безопасностью

С внедрением как облачной инфраструктуры, так и облачных сервисов (SaaS) будет происходить больше атак, адаптированных и настроенных для обхода существующих ограждений облака. По мнению Бен Дов, хакеры будут искать способы обойти механизмы облачной аутентификации.

Связанная с этим проблема связана с тенденцией компаний, разрабатывающих свои собственные внутренние приложения, превращаясь в собственную компанию по разработке программного обеспечения. Она предупредила, что это открывает двери для атак на конкретные приложения.

«Хакеры всегда будут выбирать самый простой путь, и до 2020 года использование ошибок в старых операционных системах для установки вредоносных программ или людей, занимающихся социальной инженерией, для установки вредоносного ПО на свои ноутбуки было легким путем», - добавил Чай. «С перемещением данных и серверов в облако, мы со временем увидим меньше таких атак и больше атак, сосредоточенных на облачных средах».

По словам Сицилиано, ключевым элементом, который необходимо решить, является отсутствие внимания к роли, которую должны играть сотрудники в сфере безопасности. Особенно это касается фишинга. Сотрудникам необходимо лучше понимать, как их неэффективность может привести к катастрофе.

«Тренинги по осведомленности о безопасности, поскольку они относятся к симуляции фишинга, сами по себе абсолютно недостаточны и не решат проблему. Обсуждение необходимо сместить с осведомленности о безопасности к оценке безопасности, а сейчас большинство организаций этого не делают», - пожаловался он.

Последние мысли

Главный пробел, который сегодня видит Чай в отношении безопасности и конфиденциальности данных, заключается в том, что существующие решения не

подходят для модели, которая использует правовой контекст данных. Модели для существующих инструментов защиты данных в основном черные или белые. «Либо у вас есть, либо нет доступа к данным», - пояснил он.

Однако, по его мнению, конфиденциальность и правовой контекст данных намного сложнее. Часть данных может быть авторизована для использования на основании согласия, данного при сборе данных, географического расположения данных, размера и характера набора данных, способа использования данных и ряда других соображений.

«Пока юридический контекст и контекст конфиденциальности не будут интегрированы в существующие модели защиты данных, мы все равно будем отставать», - сказал он.

Этот процесс потребует расширения сотрудничества и партнерства между отраслью, правительством и академическими кругами для обмена данными, касающимися угроз кибербезопасности. Для противодействия им также потребуются знания об угрозе, добавил Бен Дов». ***(Jack M. Germain. Is 2021 the Year Cyberattacks Force Privacy Laws to Grow Some Teeth? // ECT News Network (https://www.technewsworld.com/story/87008.html). 04.02.2021).***

***

«Штат Вирджиния может стать следующим штатом, который примет закон о конфиденциальности. Законопроект № 1392 Сената недавно был принят Сенатом и, вероятно, находится на пути к губернатору Ральфу Нортаму. Законопроект добавляет Закон о защите данных потребителей в Кодекс Вирджинии и включает определения биометрических данных, точных данных геолокации, профилирования, конфиденциальных данных и целевой рекламы. Дата вступления в силу закона - 1 января 2023 года.

Законопроект будет применяться к лицам, которые ведут бизнес в Содружестве или производят продукты или услуги, предназначенные для жителей Содружества, и которые (i) в течение календарного года контролируют или обрабатывают данные не менее 100000 потребителей или (ii) контролируют или обрабатывать персональные данные не менее 25 000 потребителей и получать более 50 процентов валового дохода от продажи персональных данных. Закон не будет применяться к государственным или местным государственным учреждениям, финансовым учреждениям, подпадающим под действие Закона Грэмма-Лича-Блайли, а также к юридическим лицам или бизнес-партнерам, подпадающим под действие Закона о переносимости и подотчетности медицинского страхования (HIPAA) и медицинских информационных технологий для Закон об экономическом и клиническом здоровье (HITECH Act).

Права потребителей включают следующее:

Право знать, обрабатывает ли контроллер персональные данные потребителя, и право на доступ к таким персональным данным;

Право на исправление неточностей в личных данных потребителя;

Право на удаление персональных данных, предоставленных или полученных о потребителе;

Право на переносимость данных; и

Право отказаться от обработки персональных данных в целях (i) целевой рекламы, (ii) продажи персональных данных или (iii) профилирования во исполнение решений, которые имеют юридические или аналогичные значимые последствия для потребителя.

Законопроект предназначен для обозначения контроллеров данных и обработчиков данных и организует права и обязанности каждого в соответствии с этими ролями. В этом законопроекте нет частного права на предъявление иска, поскольку Генеральному прокурору поручено обеспечивать соблюдение правил. Генеральный прокурор будет обладать исключительными полномочиями по обеспечению соблюдения нарушений от имени Содружества или от имени отдельных лиц, проживающих в Содружестве». ***(Deborah George. Virginia Might Be the Next State to Enact a Privacy Law // Robinson & Cole LLP (https://www.dataprivacyandsecurityinsider.com/2021/02/virginia-might-be-the-next-state-to-enact-a-privacy-law/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+DataPrivacyAndSecurityInsider+%28Data+Privacy+%2B+Security+Insider%29). 18.02.2021).***

***

«Сообщается, что Управление аудитора штата Вашингтон (SAO) расследует инцидент безопасности, предположительно вызванный сторонним поставщиком, который, возможно, скомпрометировал личную информацию до 1,6 миллиона жителей штата Вашингтон, которые подали Обращения по безработице в 2020 году.

SAO расследует мошеннические заявления о безработице, поданные в Вашингтоне в 2020 году, которые, как сообщается, обошлись штату в 600 миллионов долларов. При завершении аудита штат использовал стороннего поставщика Accellion для передачи компьютерных файлов для расследования.

Согласно SAO, «в течение недели с 25 января 2021 года Accellion подтвердил, что неавторизованное лицо получило доступ к файлам SAO, воспользовавшись уязвимостью в службе передачи файлов Accellion». SAO опубликовало на своем веб-сайте информацию о том, что неавторизованное лицо «смогло использовать уязвимость программного обеспечения в службе передачи файлов Accellion и получить доступ к файлам, которые передавались с помощью службы Accellion», что произошло в декабре 2020 года.

Данные, которые могли быть затронуты, включают 1,6 миллиона исков физических лиц, поданных в период с 1 января 2020 года по 10 декабря 2020 года, включая иски, поданные государственными служащими. Скомпрометированная информация включает имена людей, номера социального страхования и / или водительские права или государственные идентификационные номера, банковскую информацию и место работы. Кроме того, была скомпрометирована личная информация некоторых лиц, информация о которых находилась в распоряжении Департамента по делам детей, молодежи и семьи.

Какие ужасные последствия для тех, кто законно потерял работу и подал заявление на пособие по безработице. Для тех, чья личная информация была

использована для подачи мошеннического заявления о пособии на пособие по безработице, эта новость бросает серьезный удар в рану того, что они стали жертвой кражи личных данных». ***(Linn Foster Freedman. Ransomware Incident Compromises Unemployment Claim Information of 1.6M in WA // Robinson & Cole LLP (https://www.dataprivacyandsecurityinsider.com/2021/02/ransomware-incident-compromises-unemployment-claim-information-of-1-6m-in-wa/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+DataPrivacyAndSecurityInsider+%28Data+Privacy+%2B+Security+Insider%29). 04.02.2021).***

***

«13 января делегат Палаты представителей Сара Лав представила «Закон о биометрических идентификаторах и конфиденциальности биометрической информации» («Закон»), в значительной степени созданный по образцу Закона о конфиденциальности биометрической информации в Иллинойсе, 740 ILCS 14 et seq. («BIPA»). Принятый в 2008 году BIPA штата Иллинойс только недавно вызвал лавину коллективных исков в штате Иллинойс, подстегнув другую законодательную деятельность, в том числе в Нью-Йорке. В случае принятия Акт Мэриленда вступит в силу 1 января 2022 года.

Так же, как BIPA и предложенный закон в Эмпайр-Стейт, Закон установит правила для «частных лиц», обладающих «биометрическими идентификаторами» и «биометрической информацией» человека, такими как:

Разработка общедоступной политики, устанавливающей правила хранения и уничтожения,

Обязанные разумные меры предосторожности, относящиеся к хранению, передаче и раскрытию такой информации, по крайней мере, таким же образом, как и для «конфиденциальной и конфиденциальной информации», таких как номера социального страхования и номера счетов,

Запрещение частным организациям извлекать выгоду из информации, и

Ограниченное право на раскрытие информации без согласия.

В отличие от BIPA, законопроект Мэриленда разъясняет, что политика не обязательно должна быть общедоступной, если она применяется только к сотрудникам и используется только для внутренних операций.

Наиболее важно то, что Закон также создаст частное право на предъявление иска для лиц, «пострадавших» от нарушений Закона, используя формулировку, аналогичную BIPA, позволяя лицам взыскать большую из (i) установленных законом убытков в размере не менее 1000 долларов США за каждую небрежность нарушение или 5000 долларов за каждое умышленное или неосторожное нарушение, и (ii) фактический ущерб.

Мы знаем, что Верховный суд штата Иллинойс постановил, что, как правило, лицам, подающим иск в соответствии с BIPA, не нужно заявлять о фактических травмах или неблагоприятных последствиях, помимо нарушения их прав в соответствии с BIPA, для того, чтобы квалифицироваться как «потерпевшее» лицо и иметь право требовать заранее оцененных убытков, гонораров и расходов адвокатов, а также судебного запрета в соответствии с BIPA. См. Дело Розенбах против Six Flags Entertainment Corp.

Как и в случае с предложенным BPA в Нью-Йорке, закон Мэриленда еще не принят. Однако в случае его принятия частные организации, подпадающие под действие Закона, должны незамедлительно принять меры для его соблюдения. То есть они должны пересмотреть свои тайм-менеджмент, точки покупки, физическую безопасность или другие системы, которые получают, используют или раскрывают биометрические идентификаторы или биометрическую информацию, в соответствии с требованиями Закона. Биометрические идентификаторы в соответствии с Законом включают данные человека, полученные в результате автоматических измерений биологических характеристик этого человека, таких как отпечаток пальца, отпечаток голоса., генетический отпечаток, изображение сетчатки или радужной оболочки или любые другие уникальные биологические характеристики, которые могут использоваться для однозначной аутентификации личности. В этом отношении Закон будет шире, чем BIPA - в Иллинойсе биометрический идентификатор ограничен сканированием сетчатки или радужной оболочки глаза, отпечатком пальца, отпечатком голоса или сканированием геометрии руки или лица. Однако в соответствии с Законом существуют исключения из биометрических идентификаторов, таких как образцы письменных принадлежностей, фотографии, демографические данные, физические характеристики (такие как рост и вес) и защищенная медицинская информация, на которую распространяется HIPAA.

В случае, если частные организации обнаруживают технические или процедурные пробелы в соблюдении требований, такие как отсутствие политики хранения и уничтожения такой информации или получение согласия на предоставление биометрической информации третьей стороне, они должны быстро устранить эти пробелы.

Неясно, будут ли суды в Мэриленде толковать доступность средств правовой защиты в соответствии с Законом, если он будет принят, так же, как Верховный суд Иллинойса в Розенбахе. Однако, если они это сделают, обязанности, возложенные на частные лица, подпадающие под действие закона, в отношении владения, хранения, раскрытия, защиты и уничтожения биометрических идентификаторов человека или биометрической информации будут определять установленные законом права лиц, защищаемых законом. Соответственно, когда частное лицо не соблюдает одно из требований Закона, это нарушение может представлять собой вторжение, нарушение или отказ в праве, предусмотренном Законом, в результате чего лицо будет «обижено» и получит право требовать возмещения». ***(Joseph J. Lazzarotti. Maryland Joins New York with a BIPA-like Biometric Privacy Bill // Jackson Lewis P.C.. (https://www.workplaceprivacyreport.com/2021/02/articles/biometric-information/maryland-joins-new-york-with-a-bipa-like-biometric-privacy-bill/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+WorkplacePrivacyDataManagementSecurityReport+%28Workplace+Privacy%2C+Data+Management+%26+Security+Report%29#page=1). 21.02.2021).***

***

«В эпоху, когда данные становятся все более ценными, защита конфиденциальных личных данных и кибербезопасность стали приоритетными для многих корпораций. Темпы роста данных были экспоненциальными: по текущим оценкам, объем данных превышает 40 триллионов гигабайт (40 зетабайт). Учитывая растущий риск киберугроз, суды ищут подходящие средства правовой защиты от крупномасштабных утечек данных.

Истцы все чаще пытались использовать коллективные иски в качестве средства разрешения исков о нарушениях конфиденциальности. Однако в ряде из этих дел суды отказали в подтверждении потенциального группового иска (см. Наш Бюллетень Блейкса: Предлагаемый групповой иск в отношении конфиденциальности «рушится во всей своей полноте» по вопросу общности). В недавнем решении вСетогучи против Uber CV, 2021 ABQB 18 (Сетогучи), помощник председателя суда королевской скамьи Альберты, отказал в подтверждении группового иска о предполагаемом нарушении конфиденциальности. При этом суд подчеркнул свою важную роль в отсечении необоснованных исков на раннем этапе. В частности, суд подчеркнул необходимость наличия значимых доказательств ущерба или ущерба, причиненного предполагаемым нарушением конфиденциальности.

Хотя ожидается, что предполагаемые групповые иски о конфиденциальности останутся обычным явлением в Канаде в обозримом будущем для устранения заявленных нарушений конфиденциальности, решение в Сетогучи подчеркивает растущую готовность судов внимательно изучать иски истцов, чтобы определить, являются ли коллективные иски подходящим форумом для решения крупномасштабных нарушений данных.

РЕШЕНИЕ

Предлагаемый представитель истца и представители предлагаемой национальной категории были пользователями или водителями, которые использовали платформу Uber, и поэтому часть их данных хранилась в различных компаниях Uber.

Реальный вопрос в этом деле заключался в том, имелись ли, даже если предположить наличие иным образом доказуемой причины иска (в контракте, халатность, нарушение закона и т. Д.), Были ли «некоторые доказательства» или «некоторые фактические основания» для любого реального нанесенного ущерба, потеря или повреждение в результате заявленных норм общего права или установленных законом нарушений. В то время как Uber признал, что нарушение заявленных стандартов обслуживания может повлечь за собой ответственность, Uber утверждал, что для того, чтобы такие претензии были успешными, должно быть доказательство ущерба или убытков.

Оценивая информацию, которая была взломана, помощник главного судьи Рук отметил, что, хотя информация, к которой был получен доступ, была частной, она не обязательно была конфиденциальной, поскольку она включала информацию, которая была бы доступна в «типичном телефонном справочнике» прошлого.

Однако, что еще более важно, суд установил, что не только отсутствовали какие-либо доказательства ущерба или убытков, но и верно обратное, а именно, что протокол показал, что не было никакого ущерба или убытков для предполагаемого класса. Это открытие в конечном итоге оказалось фатальным при попытке сертификации предложенного группового иска. Как отметил суд, «должны быть какие-то доказательства или фактические основания для утраты или повреждения… Представитель истца должен продемонстрировать хотя бы некоторую значимую сущность дела, прежде чем должно быть предоставлено свидетельство». В противном случае, как заметил суд, планка была бы установлена настолько низкой, что практически любая корпорация, пострадавшая от утечки данных, могла бы стать объектом коллективного иска без необходимости для истцов доказывать ущерб.

Суд провел обширный обзор установленной судебной практики, связанной с утечкой данных, и опирался на ряд четко установленных принципов в отказе в сертификации. Кроме того, суд учел и включил принцип соразмерности, сформулированный Верховным судом Канады в деле Hryniak v Mauldin, 2014 SCC 7 (Hryniak), чтобы признать, что коллективный иск не является предпочтительной процедурой. Гриняк и его потомки подчеркивают важность функции суда при рассмотрении необоснованных исков на ранней стадии. Ссылаясь на Гриняка, суд заявил, что «пришло время суду серьезно отнестись к своей функции охраны ворот и прекратить этот судебный процесс как групповое разбирательство сейчас…».

ОСНОВНЫЕ ВЫВОДЫ

В решении по делу Сетогучи подчеркивается роль судов при оценке предполагаемых групповых исков и дается более тщательный анализ таких исков на ранней стадии. В частности, в решении учтены настроения Гриняка, в том числе необходимость на раннем этапе отсеять необоснованные претензии и претензии de minimis. Кроме того, решение требует, чтобы были представлены достаточные доказательства, чтобы продемонстрировать подлежащий компенсации ущерб или убыток в связи с любым заявленным нарушением, чтобы поддержать сертификацию группового иска.

Учитывая высокие ставки кибербезопасности и растущие риски, связанные с утечкой данных, подход судов к групповым искам становится все более важным вопросом. Подход суда в Сетогучипредполагает, что истцы могут столкнуться с повышенным вниманием при попытках удостоверить свои требования как групповые иски». ***(Dalton W. McGrath, Q.C., FCIArb., Birch Miller, Michael O'Brien. Uber Denial of Class Action – Alberta Court Denies Certification of Privacy Class Action // Blake, Cassels & Graydon LLP (https://www.blakes.com/insights/bulletins/2021/uber-denial-of-class-action-%E2%80%93-alberta-court-denies). 18.02.2021).***

***

«…Министерство общественной безопасности Вьетнама («MPS») недавно опубликовало долгожданный проект Указа о защите личных данных для общественных консультаций. Проект Указа впервые предлагает регулирование конкретных прав субъектов данных, трансграничной передачи

данных, обработки конфиденциальных персональных данных и других связанных тем.

В этой статье мы выделяем следующие важные моменты проекта Указа.

Руководящие принципы защиты персональных данных

Существует восемь принципов защиты личных данных («ПД»).

Законность. ПД можно получить только в необходимых случаях в соответствии с законодательством.

Назначение Ограничения. ПД могут обрабатываться только для целей, которые были зарегистрированы или заявлены.

Минимизация данных. ПД могут быть получены только в той степени, в которой это необходимо для достижения поставленной цели.

Ограничения использования. ПД может использоваться только при наличии согласия субъектов данных или когда это требуется властями.

Качество данных. ПД следует обновлять и дополнять, чтобы обеспечить его обработку.

Безопасность. Необходимо применять меры безопасности для защиты ПД от обработки.

Информированные субъекты данных. Субъекты данных имеют право знать и получать информацию о действиях по обработке своих ПД.

Конфиденциальность. ПД следует хранить в тайне во время обработки.

Некоторые из этих принципов в чем-то похожи на те, которые содержатся в Общем регламенте защиты данных («GDPR»), который включает положения о минимизации данных и ограничении целей.

Широкая и трансграничная сфера управления

Проект Указа предлагает обращаться к любой организации или физическому лицу, имеющему отношение к ПД. Это означает, что обработка данных жителей Вьетнама местными или иностранными компаниями (независимо от того, базируются ли они во Вьетнаме или нет) будет регулироваться этим Указом.

Особые права субъектов данных

Проект Указа впервые предусматривает конкретные права на обработку персональных данных. Субъекты данных имеют право:

Дать согласие на обработку своих ПД;

Получать уведомление обработчика данных во время обработки или как можно скорее;

Просить обработчика исправить, показать и предоставить копию своих ПД;

Требовать от обработчика прекратить обработку своих ПД, ограничить доступ к своим ПД, прекратить раскрытие или доступ к своим ПД, удалить или закрыть их ПД;

Подавать жалобу в Комитет по защите персональных данных в случае нарушения или неправомерного использования данных; и

Требовать возмещения ущерба в результате нарушения ПД.

Проект Указа требует согласия субъекта данных в формате, который можно распечатать или скопировать в письменной форме.

Создание комитета по защите персональных данных

В соответствии с главой IV проекта Указа для реализации этого постановления будет создан Комитет по защите персональных данных. Это новое агентство является независимым правительственным органом при Департаменте кибербезопасности и предупреждения высокотехнологичных преступлений Министерства общественной безопасности (Департамент A05). Директор Департамента A05 предлагается стать Председателем этого Комитета. Основная функция комитета включает оценку политик конфиденциальности обработчиков данных до их объявления, рассмотрение и утверждение заявок на трансграничную передачу ПД и заявок на обработку конфиденциальных данных, а также обращение к Департаменту A05 с просьбой принять решение о проверке и изучении данных. деятельность по защите и рассмотрение жалоб на нарушение или неправомерное использование данных.

Трансграничная передача данных

Указ станет первым инструментом, конкретно регулирующим эту сферу. Предлагаемые требования для трансграничной передачи данных включают (i) согласие субъекта данных; (ii) исходные данные хранятся во Вьетнаме; (iii) имеются письменные доказательства того, что юрисдикция, в которой получены данные, предлагает такой же или более высокий уровень защиты данных по сравнению с Вьетнамом; и (iv) Комитет по защите персональных данных выдал письменное разрешение на передачу.

Заявка на трансграничную передачу данных должна включать: (i) форму с подробными сведениями об обработчике данных, юридические основания для передачи, цели передачи, типы данных, которые должны быть переданы, источники данных, местоположение и условия передачи, подробное описание мер защиты; (ii) отчет об оценке воздействия трансграничной передачи данных, включая описание передачи, цели передачи, оценку рисков и вреда и меры по снижению или устранению таких рисков или вреда; (iii) документы, относящиеся к информации в заявке и отчете об оценке воздействия на обработку конфиденциальных данных. Комитет по защите персональных данных может предпринять шаги для проверки информации в приложении.

Конфиденциальные личные данные

В проекте Указа в качестве конфиденциальной информации указываются следующие типы информации: политические и религиозные взгляды; личные данные о здоровье; персональные генетические данные; личные биометрические данные; ПД по гендерному статусу; ПД о жизни, сексуальной ориентации; ПД о преступниках и преступлениях, собираемых и хранимых правоохранительными органами; личные финансовые данные; данные о личном местонахождении; ПД по социальным отношениям; другие ПД в соответствии с законодательством, требующие необходимых мер безопасности.

Обработка конфиденциальных ПД также должна быть одобрена Комитетом по защите персональных данных, при этом приложение должно включать форму и отчет об оценке воздействия, содержание которых аналогично трансграничной передаче данных.

Санкции за нарушение

В проекте Указа предлагается применить денежный штраф в размере от 50 до 80 миллионов донгов (примерно от 2170 до 3480 долларов США) за нарушения прав субъектов данных, хранение, уничтожение, раскрытие, обработку данных (в том числе с помощью автоматической означает), точность и данные, касающиеся детей. Размер денежного штрафа будет увеличен до 80–100 млн вьетнамских донгов (примерно от 3480 до 4350 долларов США) за нарушения, связанные с трансграничной передачей ПД, обработкой конфиденциальных данных и неприменением технических мер. За последние нарушения дополнительные санкции могут также включать приостановление обработки данных на срок от одного до трех месяцев и отзыв прав на обработку конфиденциальных данных и трансграничную передачу. За повторные нарушения может быть наложен денежный штраф в размере 5% от общей выручки нарушителя.

Вывод

Помимо вышеизложенного, проект Указа также охватывает:

обстоятельства, при которых ПД могут быть обработаны или раскрыты без предварительного согласия субъектов данных, автоматическая обработка ПД;

необходимые технические меры безопасности и публикация политик защиты ПД;

хранение, удаление и уничтожение ПД;

обработка ПДн в отношении детей; и

Обработка ПД для научных исследований и статистических целей.

В проекте Указа есть определенные области, которые, по-видимому, частично совпадают с другими указами (например, Указ № 52/2013 / ND-CP от 16 мая 2013 г. об электронной торговле и Указ № 72/2013 / ND-CP от 15 июля 2013 г. об управлении, предоставлении и использовании интернет-сервисов и онлайн-информации), а также находящегося на рассмотрении проекта указа, регулирующего выполнение вьетнамского закона о кибербезопасности. Еще предстоит увидеть, как МОБ устранит различия между проектом Указа и другими существующими правовыми инструментами. MPS стремится доработать проект и представить его в Правительство в течение первого квартала 2021 года». ***(Yen Vu. Vietnam: Draft Decree on Personal Data Protection Issued for Public Consultation // Rouse International Limited (https://rouse.com/insights/news/2021/vietnam-draft-decree-on-personal-data-protection-issued-for-public-consultation). 16.02.2021).***

***

«Стены для встреч и чаты Zoom, приложения для отслеживания COVID и требования к работе из дома в 2020 году подняли проблемы технологий и конфиденциальности на совершенно новый уровень осознания в нашем бизнесе и частной жизни.

В сочетании с вступившим в силу в Новой Зеландии Законом о конфиденциальности 2020 года и продолжающимися глобальными тенденциями в отношении суровых наказаний для лиц, нарушающих законы о защите данных, в 2021 году Новая Зеландия, похоже, наконец присоединится к маршу к большей конфиденциальности и управлению киберрисками и обеспечению соблюдения.

Уже несколько лет мы наблюдаем экспоненциальный рост объемов сбора, хранения и обработки данных в новозеландских организациях. Технологический бум 2020 года, связанный с работой на дому, только усугубил этот рост, как в отношении личной информации, так и ценных коммерческих данных. Чтобы справиться с объемами и требованиями рынка, предприятия постепенно перешли на цифровые платформы, решения для электронной коммерции и цифровые хранилища информации. Темпы этого перехода не замедляются.

Поэтому неудивительно, что кибератаки и утечки данных стали регулярными новостями. CERT NZ сообщил о 3102 «инцидентах кибербезопасности» за шесть месяцев до конца июня 2020 года; рост на 42% по сравнению с аналогичным периодом прошлого года. Только в апреле 2020 года (когда Новая Зеландия находилась в изоляции) было получено 820 сообщений об инцидентах. Это был самый высокий ежемесячный объем отчетов об инцидентах с момента создания агентства в 2017 году. В третьем квартале 2020 года CERT получил в общей сложности 2610 отчетов об инцидентах, что на 33% больше, чем во втором квартале.

С учетом Закона о конфиденциальности 2020 года мы ожидаем увидеть ощутимое увеличение в течение следующих 12-24 месяцев действий по обеспечению конфиденциальности в Новой Зеландии. Это, в частности, является результатом обязательной отчетности о нарушениях и других механизмов обеспечения соблюдения, призванных наделить более широкими полномочиями регулирующий орган Новой Зеландии - Управление уполномоченного по вопросам конфиденциальности. Реформы увеличивают судебный риск для новозеландских агентств и любого агентства, ведущего бизнес в Новой Зеландии, и повлияют на то, как организации, ведущие бизнес в Новой Зеландии, решают вопросы конфиденциальности и безопасности данных.

Мировые тенденции

Если зарубежные тенденции будут повторяться в Новой Зеландии, Офис уполномоченного по вопросам конфиденциальности будет вынужден отказаться от своей работы.

Австралия

В Австралии Управление Комиссара по информации Австралии (OAIC) сообщило об увеличении количества уведомлений в соответствии с их схемой обнаружения утечек данных на 11% с 2018-2019 (950) по 2019-2020 (1050). OAIC также впервые в этом году инициировал гражданский иск против Facebook за приложение This is Your Digital Life.

Объединенное Королевство

В Великобритании Управление комиссара по информации (ICO) наложило два самых крупных штрафа за утечку данных в истории Великобритании. 16 октября 2020 года ICO оштрафовала British Airways на 20 миллионов фунтов стерлингов (25,8 миллиона новозеландских долларов). Две недели спустя, 30 октября 2020 года, ICO оштрафовало Marriott на 18,4 миллиона фунтов стерлингов (23,7 миллиона новозеландских долларов).

Штраф British Airways представляет собой самый крупный штраф, наложенный на сегодняшний день за нарушение Общего законодательства о

защите данных (GDPR). Однако штрафы British Airways и Marriott представляют собой снижение почти на 90% и 81% соответственно от предложенных штрафов. Это демонстрирует, что ICO желает снизить штрафы, если организации демонстрируют эффективные меры по смягчению последствий и корректирующие действия. Регулирующие органы в других юрисдикциях не проявили такого дружеского подхода. В Германии компания H&M недавно получила штраф в размере 35 миллионов евро за чрезмерное наблюдение за сотрудниками в ее сервисном центре в Нюрнберге.

Регуляторное сотрудничество

Штрафы в соответствии с нашим Законом о конфиденциальности существенно меньше, чем в других юрисдикциях (максимальная сумма новых финансовых санкций составляет 10 000 новозеландских долларов). Это делает вероятным, что мы увидим разумный уровень сотрудничества между регулирующими органами Новой Зеландии в отношении подхода к конфиденциальности и кибербезопасности, чтобы оправдать ожидания общественности в отношении законов о защите данных.

В прошлом году мы отметили, что Комиссия по торговле начинает уделять внимание нарушениям конфиденциальности как проблеме защиты потребителей. На первом саммите Международной ассоциации профессионалов в области конфиденциальности Австралии и Новой Зеландии в Сиднее (в 2019 году) комиссар по конфиденциальности признал, что здесь одних законов о защите данных может быть недостаточно для борьбы с потенциальным вредом. Он поинтересовался, нужны ли нам более гибкие механизмы защиты потребителей, чтобы регуляторы конфиденциальности могли работать вместе с регуляторами безопасности потребителей. У Комиссии по торговле, безусловно, есть возможности для гибкости своих правоприменительных полномочий, чтобы гарантировать, что личная информация потребителей не используется вводящими в заблуждение или вводящими в заблуждение способами в соответствии с Законом о добросовестной торговле.

Кроме того, Уполномоченный по вопросам конфиденциальности может обратиться к Управлению по финансовым рынкам (FMA) за поддержкой в вопросах правоприменения и обеспечения того, чтобы агентства, регулируемые FMA, применяли разумные методы обеспечения конфиденциальности для защиты как организаций, так и потребителей финансовых продуктов. В течение последних 12 месяцев мы наблюдали некоторую активность в этой области: FMA выпускает уведомления по разделу 25 для сбора информации о методах обеспечения конфиденциальности и кибербезопасности.

Австралия уже предприняла шаги в этом направлении, когда Австралийская комиссия по ценным бумагам и инвестициям (ASIC) возбудила дело в Федеральном суде Австралии против RI Advice Group Pty Ltd (RI), владельца лицензии на финансовые услуги Австралии (AFS), за то, что иметь адекватные системы кибербезопасности. ASIC утверждает, что Frontier Financial Group, уполномоченный представитель RI, подверглась атаке методом «грубой силы», в результате которого злоумышленник успешно получил удаленный доступ к серверу Frontier и провел более 155 часов, авторизовавшись на сервере, который

содержал конфиденциальную информацию о клиенте, включая документы, удостоверяющие личность. ASIC утверждает, что RI не смогла реализовать адекватные политики, системы и ресурсы, которые были разумно подходящими для управления рисками в отношении кибербезопасности и киберустойчивости.

ASIC добивается заявлений о том, что RI нарушила положения Закона о корпорациях, а также распоряжений о соблюдении требований о том, что RI внедряет системы, которые разумно подходят для адекватного управления рисками в отношении кибербезопасности и киберустойчивости, и предоставляет отчет независимого эксперта с соответствующей квалификацией, подтверждающий, что такие системы были реализованы.

Стратегический фокус

Управление уполномоченного по вопросам конфиденциальности вступило в 2021 год (и далее) с обновленной направленностью и увеличением ресурсов для соответствия. Мы ожидаем, что сначала будет сфокусировано двойное образование / судебное разбирательство (с упором на образование, в частности, в 2021 году), что даст агентствам некоторое время, чтобы адаптироваться к требованиям Закона о конфиденциальности.

Однако мы ожидаем, что Уполномоченный по вопросам конфиденциальности будет стремиться убедительно заявить о соблюдении и искать соответствующие случаи для обеспечения соблюдения новых стандартов Закона. Мы также предполагаем, что Комиссар будет работать с другими, более серьезными регулирующими органами, чтобы гарантировать, что агентства, ведущие бизнес в Новой Зеландии, соблюдают свои обязательства в отношении конфиденциальности, а также являются кибербезопасными и устойчивыми». ***(2021 Litigation Forecast - Cyber and privacy risk: Back in the spotlight // MinterEllisonRuddWatts (https://www.minterellison.co.nz/our-view/2021-litigation-forecast-cyber-and-privacy-risk-back-in-the-spotlight). 11.02.2021).***

***

«Европейский совет по защите данных («EDPB») опубликовал дополнительные руководящие принципы («Указания») к существующим руководящим указаниям по уведомлению об утечке персональных данных, выпущенным его предшественницей Рабочей группой по статье 29. Руководящие принципы включают 18 тематических исследований, основанных на коллективном опыте органов по защите данных ЕС, охватывающих утечки данных, связанные с программами-вымогателями, атаками с кражей данных, человеческими ошибками или рисками, потерей устройств или документов, ошибками публикации и социальной инженерией. Кроме того, в Руководстве изложено обоснование необходимости уведомления субъектов данных и / или надзорных органов в отношении нарушений в каждом конкретном исследовании, а также предложены меры по смягчению последствий и передовой опыт после утечки данных.

Зачем нужны Руководящие принципы и актуально для британского бизнеса

Существующее руководство по уведомлению об утечке данных появилось раньше Общих правил защиты данных (GDPR). В течение двух с половиной лет с GDPR был реализован, многие контролирующие органы испытали завышая

потенциальные нарушения данных, но некоторые из наиболее серьезных нарушений не были зарегистрированы в кратчайших сроках. Пандемия COVID-19 также ускорила технологическую трансформацию почти во всех секторах, что привело к повышению рисков кибербезопасности и конфиденциальности. Таким образом, обновленные, обновленные и основанные на сценариях руководящие принципы, отражающие меняющийся ландшафт кибербезопасности и утечки личных данных, будут приветствоваться предприятиями и организациями государственного сектора в ЕС и Великобритании.

Несмотря на то, что Великобритания вышла из Европейского Союза, британские компании, попавшие в экстратерриториальный охват GDPR, например, нацеленные на субъектов данных ЕС и продажу им товаров или услуг, все равно должны будут соблюдать GDPR. Персональные данные субъектов данных ЕЭЗ, собранные до 31 декабря 2020 года, также продолжают регулироваться GDPR в том виде, в каком он действовал на эту дату. Даже в отношении личных данных, обнаруженных только теперь британской версией GDPR, британское ICO признало, что большинство ранее существовавших руководящих принципов EDPB остаются полезными и убедительными для британского режима и во избежание риска того, что Великобритания не получит адекватность. По решению ЕС, Великобритания, вероятно, в краткосрочной перспективе воспользуется аналогичными подходами к руководствам EDPB на практике.

Основные выводы из Руководства

Поскольку Руководящие принципы основаны на сценариях, каждый сценарий содержит нюансы в своей фактической матрице. Таким образом, Руководство стоит внимательно прочитать профессионалам в области защиты данных и DPO. Однако в Руководстве представлены несколько общих тем, которые мы кратко изложили ниже.

Руководство актуально для принудительных действий: Сфера применения Руководства распространяется на шаги по смягчению последствий, которые могут предпринять предприятия, и меры безопасности, которые должны быть реализованы после утечки данных, а это означает, что Руководство также может иметь значение, когда надзорные органы определяют, были ли приняты соответствующие меры безопасности при принятии решения о мерах по обеспечению соблюдения. В частности, EDPB подчеркнула важность наличия в организациях соответствующих процедур защиты от нарушений и еще раз подчеркнула важность регулярных учебных занятий. EDPB также отметил, что Контроллеры, работающие с конфиденциальными данными (включая финансовую информацию), несут более высокую степень ответственности за обеспечение безопасности обрабатываемых персональных данных и что несоблюдение этих более высоких стандартов приведет к более серьезным мерам, принимаемым надзорными органами.

Рассмотрим влияние утечки данных на конфиденциальность, целостность и доступность данных: на протяжении всего Руководства EDPB рассматривал влияние каждой утечки данных на эти три аспекта затронутых данных. В большинстве случаев нарушение конфиденциальности данных может привести к более высоким рискам, чем простое нарушение доступности. В Руководящих

принципах приводятся примеры, когда простая недоступность данных может вызвать обязательства по уведомлению в соответствии с GDPR. Например, считается, что недоступность медицинских записей может привести к существенным последствиям для затронутых субъектов данных (например, задержка в лечении) и, следовательно, может привести к возникновению обязательств по уведомлению GDPR.

Факторы, имеющие значение для определения того, является ли нарушение высоким риском и поэтому о нем следует уведомлять, не являются исчерпывающими, однако мы определили следующие моменты, которые следует отметить:

характер, объем и контекст затронутых персональных данных и потенциальное влияние на субъектов данных: например, потеря данных специальной категории, данных, раскрывающих личную жизнь человека, или данных, которые могут привести к краже личных данных или финансовым потерям субъекта данных. более вероятно, что возникнут обязательства по уведомлению.

характер несанкционированного доступа имеет значение: например, были ли данные, к которым был получен доступ без авторизации, также были скопированы или отфильтрованы. В целом считается, что несанкционированный доступ без утечки менее опасен.

были ли скомпрометированные данные зашифрованы с использованием современных технологий, был ли скомпрометирован ключ расшифровки, а в случае паролей применялись ли криптографическое хеширование и соление. Если такие технические меры не приняты, утечка данных с большей вероятностью создаст более высокий риск для людей.

можно ли смягчить неблагоприятный эффект утечки данных в пределах сроков срочного уведомления: например, путем восстановления скомпрометированных данных из хорошо обслуживаемых резервных копий в пределах 72-часового срока для уведомления о взломе данных. Трудности с восстановлением скомпрометированных данных в течение такого периода увеличивают риски, которые нарушение данных представляет для соответствующих субъектов данных». ***(David Varney, Yunzhe Zhang. EDPB publishes detailed guidelines on data breach notification // Burges Salmon (https://www.burges-salmon.com/news-and-insight/legal-updates/data-protection/edpb-publishes-detailed-guidelines-on-data-breach-notification/). 08.02.2021).***

***

«TikTok снова в центре внимания из-за того, как популярное приложение для обмена видео собирает и передает данные, особенно от несовершеннолетних пользователей.

Зонтичная группа, состоящая из 44 организаций по надзору за конфиденциальностью потребителей, подала жалобу на TikTok, заявив, что чрезвычайно популярная платформа обмена видео имеет «вводящую в заблуждение» политику сбора данных.

Популярность TikTok, принадлежащего ByteDance, резко возросла: более 2 миллиардов загрузок на торговых площадках Google Play и Apple App Store.

Жалоба была подана Европейской организацией потребителей (BEUC), в которую входят группы по надзору за соблюдением конфиденциальности потребителей из 32 стран. BEUC заявляет, что его цель - обеспечить принятие Европейским союзом политических решений, направленных на «улучшение жизни потребителей».

Согласно жалобе, отсутствие TikTok о прозрачности сбора данных - в частности, как это влияет на большой ювенильный пользователей системы на данной платформе - это, возможно, в нарушение ЕС Общие данные Регулирование защиты (GDPR) конфиденциальности данных правил. Жалоба была подана в Европейскую комиссию (исполнительную ветвь Европейского Союза, отвечающую за внесение предложений в законодательство и выполнение решений) и в «сеть органов по защите прав потребителей».

«TikTok четко не информирует своих пользователей, особенно детей и подростков, о том, какие персональные данные собираются, с какой целью и по какой юридической причине», - говорится в отчете BEUC, опубликованном во вторник вместе с жалобой. «Эти методы проблематичны, в частности, поскольку они не позволяют потребителям принимать полностью информированное решение о том, регистрироваться ли в приложении и / или осуществлять свои права в соответствии с GDPR».

Представитель TikTok сообщил Threatpost, что внутреннее резюме Политики конфиденциальности TikTok было разработано «со словарным запасом и тоном голоса, которые помогают подросткам понять наш подход к конфиденциальности».

«Мы всегда открыты, чтобы услышать, как мы можем улучшить ситуацию, и мы связались с BEUC, поскольку мы приветствуем встречу, чтобы выслушать их опасения», - сказал Threatpost представитель TikTok.

TikTok: Политика сбора «неясных» данных

В жалобе утверждается, что условия использования и политика конфиденциальности TikTok содержат нечеткие заявления о конфиденциальности о том, как он собирает и передает данные. Например, политика конфиденциальности TikTok не предоставляет «точный список» компаний, которые получают данные, которые TikTok собирает и передает (помимо указания, что данные передаются широким категориям поставщиков облачных хранилищ, бизнес-партнеров, служб модерации контента и т. Д.).

Другие детали не указаны в политике конфиденциальности TikTok, сказал BEUC - например, он не предоставляет информацию о странах, в которые передаются данные (кроме указания, что данные будут храниться в месте назначения за пределами «Европейской экономической зоны».); и на каком правовом основании обрабатываются данные о местоположении.

BEUC также утверждает, что политика конфиденциальности TikTok (особенно для пользователей в возрасте от 13 до 18 лет) труднодоступна. Например, для доступа к политике конфиденциальности пользователи должны иметь существующую учетную запись - это означает, что «важная информация не предоставляется детям и подросткам при регистрации и на преддоговорной стадии», - говорится в сообщении BEUC.

Влияние на базу молодых пользователей TikTok

В отчете подчеркивается, что большую часть пользовательской базы TikTok составляют дети. Например, в США отчет показал, что более трети ежедневных пользователей TikTok составляют 14 лет и младше, причем многие видео, по всей видимости, исходят от детей младше 13 лет.

Таким образом, TikTok должен «четко информировать своих пользователей, особенно в понятной для детей и подростков форме, о том, какие персональные данные собираются, с какой целью и по каким юридическим причинам», согласно BEUC.

«Мы считаем, что некоторые из этих, а также другие… практики потенциально нарушают Общие правила защиты данных и привлекли к ним внимание органов по защите данных в контексте их текущих расследований в отношении компании», - заявили в BEUC.

TikTok ранее оказался в горячей воде, когда дело касалось его более молодой пользовательской базы. В мае группа защитников конфиденциальности подала жалобу в Федеральную торговую комиссию (FTC), утверждая, что платформа не в состоянии должным образом защитить конфиденциальность детей.

Но платформа социальных сетей также стремилась улучшить конфиденциальность для своих пользователей-подростков, изменив настройки конфиденциальности для всех зарегистрированных учетных записей в возрасте до 16 лет, чтобы они были конфиденциальными по умолчанию. Ограничено приложение TikTok для пользователей младше 13 лет также был запущен в прошлом году и в партнерстве с родительским сторожевой группы здравого смысла в попытке доставить соответствующие видео для молодых TikTok-ERS.

«Обеспечение безопасности нашего сообщества, особенно наших молодых пользователей, и соблюдение законов, в которых мы работаем, - это обязанности, к которым мы относимся невероятно серьезно», - сказал Threatpost представитель TikTok. «Каждый день мы усердно работаем над защитой нашего сообщества, поэтому мы предприняли ряд важных шагов, в том числе сделали все учетные записи, принадлежащие пользователям младше 16 лет, по умолчанию приватными».

Другие работы в TikTok, описанные наблюдателями конфиденциальности

В жалобе был описан ряд других проблем с приложением TikTok, выходящих за рамки его политики конфиденциальности. Например, BEUC утверждает, что TikTok не очень хорошо делает маркетинговые усилия очевидными для своей более молодой пользовательской базы. Кроме того, он потенциально неспособен проводить должную осмотрительность, когда дело доходит до защиты детей от неприемлемого контента, такого как видеоролики, демонстрирующие непристойный контент, утверждает BEUC.

BEUC также не согласился с «политикой виртуальных предметов» TikTok, согласно которой пользователи могут покупать монеты, которые они могут использовать в качестве виртуальных подарков для знаменитостей TikTok, выступления которых им нравятся. TikTok заявляет о своем «абсолютном праве» изменять обменный курс между монетами и подарками, что, по мнению BEUC, «вводит в заблуждение» и потенциально может позволить компании исказить финансовые транзакции в свою пользу.

Наконец, условия обслуживания TikTok «неясны, двусмысленны и отдают предпочтение TikTok в ущерб его пользователям», - заявили в BEUC. «Условия его авторского права также несправедливы, поскольку они дают TikTok безотзывное право использовать, распространять и воспроизводить видео, опубликованные пользователями, без вознаграждения», - говорится в сообщении BEUC.

Что ждет TikTok дальше

В рамках своей жалобы BEUC требует, чтобы власти начали всестороннее расследование политики и практики TikTok.

«Вместе с нашими членами - группами потребителей со всей Европы - мы призываем власти принять незамедлительные меры», - говорится в заявлении генерального директора BEUC Моник Гойенс. «Они должны действовать сейчас, чтобы убедиться, что TikTok - это место, где потребители, особенно дети, могут развлекаться, не будучи лишенными своих прав».

TikTok ранее подвергался критике из-за различных проблем с безопасностью и конфиденциальностью - даже в прошлом году столкнулся с угрозой запрета в Соединенных Штатах из-за опасений, что приложение тайно собирает данные о государственных служащих и подрядчиках США для использования в кибер-деятельности Китая против Соединенные Штаты.

Уязвимость в TikTok, обнаруженная в январе, могла позволить злоумышленникам легко собирать телефонные номера пользователей, уникальные идентификаторы пользователей и другие данные, готовые для фишинговых атак. В сентябре исследователи обнаружили четыре серьезных недостатка в Android-версии TikTok, которые могли быть легко использованы внешне безобидным сторонним Android-приложением.

Что касается конфиденциальности, то в августе было обнаружено, что TikTok собирает уникальные идентификаторы с миллионов устройств Android без ведома их пользователей, используя тактику, ранее запрещенную Google, поскольку это нарушало конфиденциальность людей.

«TikTok идет по проторенному пути других продуктов социальных сетей, которые имеют доступ к огромным объемам личной информации и имеют ограниченные оправдания, кроме законных интересов, которые часто упоминаются как ответ на GDPR, но становятся более сложными, когда данные не поступают» Они касаются взрослых», - сказал Threatpost Эндрю Барратт, управляющий директор отдела решений и расследований Coalfire. «В конечном итоге было бы полезно, если бы регулирующие органы использовали подход к конфиденциальности, основанный на стандартах, а не сложную договорную и юридическую позицию», - добавил он». ***(Lindsey O'Donnell. Complaint Blasts TikTok's 'Misleading' Privacy Policies // Threatpost (https://threatpost.com/tiktok-complaint-data-collection/163991/). 16.02.2021).***

***

«Компания Jones Day, которая представляла Трампа, заявила, что подвергается атаке Accellion с декабря.

Группа вымогателей Clop, как сообщается, начала публиковать данные в Dark Web, очевидно, украденные у юридической фирмы Jones Day, которая представляет

многих из самых влиятельных людей мира, включая бывшего президента Дональда Трампа, в его усилиях по отмене выборов 2020 года.

Но атака не имела ничего общего с политикой, сказал Vice человек, утверждающий, что он из хакерской группы. На вопрос о мотивации они ответили: «А как вы думаете? ☺ финансовые, конечно».

Сайт DataBreached.net первым сообщил об инциденте и опубликовал скриншоты украденных файлов Jones Day, которые группа Clop разместила в Dark Web в качестве доказательства того, что у нее есть товары. Группа сообщила DataBreaches.net, что не шифровала файлы, а просто крала копии информации. Команда Clop также сообщила, что Jones Day не ответила на ее запросы.

«Привет, они игнорируют нас, поэтому будут опубликованы», - сообщил DataBreaches.net, что группа ответила.

Предполагаемый хакер-вымогатель Clop сообщил Wall Street Journal, что 3 февраля Jones Day был уведомлен о краже данных, и по состоянию на вторник Clop не получил известий от фирмы и не обсуждал какие-либо выплаты выкупа.

Jones Day не ответил на запрос Threatpost о комментарии.

Accellion FTA нарушение

Группа вымогателей утверждает, что украла информацию непосредственно с серверов Jones Day, но фирма отрицала это в Wall Street Journal, вместо этого указывая на широко распространенную компрометацию файловой службы FTA от Accellion, которая стала точкой атаки в декабре прошлого года.

Журнал добавил, что юридическая фирма Goodwin Procter LLP также была скомпрометирована в результате взлома Accellion. Несколько других транснациональных компаний, использующих службу передачи файлов Accellion, также были скомпрометированы, в том числе оператор связи первого уровня Singtel и австралийская телекоммуникационная компания Optus.

Accellion сообщила, что 23 декабря ей стало известно об уязвимости нулевого дня в своей системе 20-летней давности, но после того, как компания подверглась атаке, последовал каскад ошибок. Но к февралю компания заявила, что система полностью исправлена.

«Accellion проводит полную оценку инцидента с безопасностью данных FTA с ведущей в отрасли фирмой по криминалистике кибербезопасности», - говорится в заявлении компании в ответ на запрос Threatpost о взломе Jones Day. «Мы поделимся дополнительной информацией, когда эта оценка будет завершена. В целях их защиты мы не комментируем конкретных клиентов. Мы работаем со всеми затронутыми клиентами FTA, чтобы понять и смягчить любые последствия этого инцидента, а также как можно скорее перенести их на нашу современную платформу брандмауэра для контента Kiteworks»

Wall Street Journal сообщил, что он проверил украденные Клопом файлы Jones Day, которые включали «файлы конфигурации и журналы Accellion со ссылками на электронную почту и веб-адреса Jones Day», а также несвязанные файлы, украденные из больницы в Калифорнии в 2016 году.

Уязвимая цепочка поставок программного обеспечения

Но Ламар Бейли, старший директор по исследованиям безопасности в Tripwire, сказал Threatpost, что, возможно, хакеры обнаружили еще одну уязвимость.

«Если «Джонс Дэй» опубликует результаты расследования, которое все еще продолжается, это должно указать на причину», - сказал Бейли. «Возможно, злоумышленник действующий, и «Джонс Дэй» еще не обнаружил первопричину, но это еще предстоит доказать».

Тем не менее, добавил Бейли, это должно служить предупреждением для организаций, чтобы они начали более пристально смотреть на свои цепочки поставок программного обеспечения.

«Старая поговорка «цепь настолько сильна, насколько ее самое слабое звено» справедливо и для сегодняшних обширных цепочек поставок», - сказал Бейли. Если один из продуктов, используемых организацией, будет эксплуатироваться, это также сделает организацию уязвимой».

Бейли рекомендует использовать упреждающие службы анализа угроз для быстрого обнаружения и устранения угроз.

«Когда предупреждение получено быстро, оцените, используются ли уязвимые версии оборудования или программного обеспечения, и примите меры по исправлению положения», - пояснил Бейли. «Если поставщик был взломан, оцените, какой доступ поставщик имел в сети и какие данные были доступны, а затем примите меры, чтобы заблокировать его, пока не будут приняты меры».

Вероятно больше жертв взлома Accellion

Ниам Малдун, специалист по глобальной защите данных в OneLogin, сказал, что это, вероятно, не будет последним из последствий взлома Accellion.

«В ближайшие месяцы мы, вероятно, увидим больше случаев раскрытия информации о нарушениях, связанных с утечкой данных Accellion, - сказал Малдун.

Малдун объяснил, что для компаний, ставших жертвами компромисса, крайне важно вести прозрачную коммуникацию с партнерами и клиентами о потенциальных рисках.

«Руководители бизнеса могут принять соответствующие меры уже сейчас, чтобы поддержать доверие своих клиентов, партнеров и сотрудников», - добавил Малдун. «Они могут добиться этого, проведя комплексную проверку своей организации, чтобы понять, используется ли инструмент обмена файлами данных Accellion и / или использовался ли он в прошлом. Открытость для клиентов, партнеров и сотрудников в отношении использования этого инструмента и потенциального воздействия позволяет принимать соответствующие меры». ***(Becky Bracken. Stolen Jones Day Law Firm Files Posted on Dark Web // Threatpost (https://threatpost.com/stolen-jones-day-law-firm-files-posted/164066/). 17.02.2021).***

***

«Около 3,27 миллиарда украденных учетных записей были опубликованы в англоязычном сообществе RaidForums, занимающемся киберпреступностью, в коллекции «COMB».

По словам исследователей, в киберподполье просочилась «компиляция множества взломов» - сокращенно COMB. Так называемый COMB содержит ошеломляющие 3,27 миллиарда уникальных комбинаций адресов электронной почты и паролей в открытом виде.

Это совокупная база данных, которая объединяет старые украденные данные из прошлых нарушений, включая учетные данные из Netflix, LinkedIn, Exploit и других. COMB, название которому дал человек, разместивший его в Интернете, впервые был обнародован 2 февраля пользователем с именем Singularity0x01, сообщил Threatpost исследователь.

«2 февраля 2020 года пользователь Singularity0x01 создал ветку на популярном англоязычном форуме киберпреступников RaidForums под названием «Compilation of Many Breaches (COMB) 3,8 миллиарда (общедоступная)», - Иван Риги, аналитик по киберугрозам из Digital Shadows, сказал.

Он добавил: «Singularity0x01 заявил, что коллекция была создана на основе предыдущей компиляции, которая содержала 1,4 миллиарда записей, и что ее содержимое было в основном общедоступным. Пользователь также сказал, что данные были представлены в алфавитном порядке и в древовидной структуре».

Он добавил, что для просмотра ссылки для загрузки защищенного паролем файла.ZIP, содержащего данные, пользователей форума попросили потратить 8 кредитов RaidForums (около 2 долларов). Затем они могут использовать встроенный в базу данных инструмент для запроса и сортировки информации, чтобы разрезать и разрезать данные.

Насколько серьезен дамп данных COMB?

Риги отметил, что сами данные не очень хорошо воспринимались обитателями подполья.

«Некоторые пользователи утверждали, что файлы были повреждены, файлы отсутствовали, общее количество учетных данных было меньше, чем заявлено, и данные были низкого качества», - пояснил он, - все это привело к тому, что Singularity0x01 получил отрицательную репутацию на криминальном форуме.

«Singularity0x01 также создал две идентичные темы на форуме, в результате чего некоторые пользователи тратят свои токены дважды», - сказал исследователь. «Singularity0x01 был навсегда заблокирован на RaidForums 8 февраля 2021 года за «утечку скрытого контента», хотя модераторы сайта не предоставили никакой дополнительной информации».

Дастин Уоррен, старший исследователь безопасности в SpyCloud, также изучил данные и определил, что комбинации входа в систему уже некоторое время циркулируют в Dark Web.

«Число 3,2 миллиарда само по себе выглядит ошеломляющим, но мы должны помнить «качество против количества», - сказал он Threatpost. «Данные, похоже, содержат учетные данные, которые были частью ранее известных нарушений. Фактически, это похоже на переиздание утечки Collection Combos из 2019 года, списка Anti Public Combo из 2016 года и, возможно, других, но выпущенного с некоторыми инструментами для дедупликации, сортировки и анализа данных, чтобы упростить использовать. Другими словами, здесь нет ничего нового».

Атаки с заполнением верительных грамот в ближайшее время

Данные могут быть старыми, но они не лишены ценности. Благодаря повторному использованию пароля хакеры могут использовать данные для проведения атак методом перебора или подбора учетных данных, чтобы захватить любое количество типов учетных записей. И оттуда потенциальные последствия становятся заметными.

«Это важное напоминание о том, что старые пароли могут возвращаться и преследовать пользователей, которые повторно используют их в разных учетных записях, поэтому даже старые данные могут быть полезны преступникам», - сказал Уоррен. «Злоумышленники, несомненно, проводят атаки с заполнением учетных данных с этими данными, поэтому любые учетные записи, использующие те же логины и пароли, все еще могут оказаться под угрозой».

Интернет-банкинг, социальные сети, порталы для пациентов, учетные записи для бонусных баллов и т. Д. - все содержат огромное количество информации, которая может быть использована, например, для финансового мошенничества или для проведения убедительной последующей фишинг-атаки. Кроме того, скомпрометированные рабочие входы и учетные записи электронной почты могут привести к попыткам шпионажа или компрометации корпоративной электронной почты (BEC).

Как предотвратить атаки COMB и пароля

Как всегда, реализация многофакторной аутентификации (MFA) и поддержание хорошей гигиены паролей (надежные, уникальные пароли для всех учетных записей и регулярная ротация паролей) могут предотвратить большую часть потенциальных последствий от этого инцидента.

«Значительное число взломов по-прежнему связано со слабыми паролями и отсутствием MFA», - сказал Threatpost Теренс Джексон, директор по информационной безопасности Thycotic. «Использование диспетчера паролей и MFA по-прежнему являются двумя из лучших способов защиты онлайн-учетных записей от атак методом подбора пароля и взлома пароля. Эти «ключи от королевства» - это то, чего жаждут злоумышленники, потому что они дают им возможность сеять хаос».

«Хотя MFA может предотвратить прямое использование учетных данных в таких службах, как Office 365, важно помнить, что MFA - не серебряная пуля.

«Простые учетные данные все равно будут полезны в сочетании с некоторыми другими скомпрометированными активами, поскольку это позволит злоумышленнику преодолеть MFA», - сказал Threatpost Оливер Таваколи, технический директор Vectra. «Конечно, это указывает на важность включения (и требования) MFA для любой проверки подлинности - особенно для служб (таких как Office 365), напрямую доступных из Интернета». ***(Tara Seals. Billions of Passwords Offered for $2 in Cyber-Underground // Threatpost (https://threatpost.com/billions-passwords-cyber-underground/163738/). 08.02.2021).***

***

«До 100 000 клиентов сервиса потоковой передачи музыки могут столкнуться с захватом аккаунтов.

Поклонники потоковой музыки Spotify оказались под прицелом еще одной кибератаки, наполненной учетными данными, всего через три месяца после последней. Служба принудительно сбросила пароли для затронутых пользователей.

Киберпреступники, выполняющие ввод учетных данных, используют людей, которые повторно используют одни и те же пароли для нескольких учетных записей в Интернете. Злоумышленники просто создают автоматизированные скрипты, которые систематически проверяют украденные идентификаторы и пароли (полученные в результате взлома другой компании или веб-сайта или купленные в Интернете) для различных типов учетных записей.

Киберпреступники успешно использовали этот подход для кражи данных у клиентов различных популярных компаний, в том числе таких громких имен, как North Face, Dunkin Donuts (который также дважды пострадал за три месяца) и популярной сети закусочных Nando's. А в прошлом году официальный аккаунт футбольного клуба «Барселона» в Твиттере был взломан в результате очевидной атаки по подбору учетных данных.

Replay: Вторая атака с заполнением учетных данных для Spotify

Еще в ноябре киберпреступники атаковали сотни тысяч пользователей Spotify, используя этот подход, в результате чего служба потоковой музыки отправила уведомления о сбросе пароля.

Исследователь Боб Дьяченко написал в Твиттере о новой атаке Spotify в четверг: «Я обнаружил вредоносную базу данных регистратора #Spotify, в которой были использованы и скомпрометированы более 100 тысяч данных учетной записи (просочившиеся в другом месте в Интернете) в рамках атаки с заполнением учетных данных».

Он также опубликовал заявление Spotify об инциденте, подтверждающее атаку.

«Недавно мы защитили некоторых наших пользователей от [атаки с заполнением учетных данных]», - говорится в уведомлении. «Как только нам стало известно о ситуации, мы сбросили пароли для всех затронутых пользователей, что сделало общедоступные учетные данные недействительными».

Компания также отметила, что атаки проводились с использованием незаконно полученного набора данных: «Мы работали над удалением мошеннической базы данных у провайдера, на котором она размещена».

Киберпреступники тоже неправильно настраивают облако

Во время первого инцидента со Spotify в ноябре исследователи обнаружили неверно настроенную и открытую облачную базу данных Elasticsearch, содержащую более 380 миллионов индивидуальных записей, включая учетные данные для входа и страны проживания для различных людей, которые активно проверяются на учетные записи Spotify. Исследователи заявили, что база данных принадлежала злонамеренной третьей стороне.

Эта вторая атака очень похожа, при этом данные для входа также отображаются в общедоступном экземпляре Elasticsearch.

«Есть сходства, но этот выглядит по-другому, как будто из конкурирующей группы», - написал Дьяченко в Твиттере. Он сказал Threatpost через Twitter DM, что наборы данных были уникальными для этой атаки.

«Первоначально эти данные были раскрыты внутри неправильно настроенного (таким образом общедоступного) кластера Elasticsearch, который, скорее всего, управлялся самими злоумышленниками», - сказал он. «Он содержал полные журналы их операций, а также пары электронной почты / пароля, которые они использовали [для атаки]».

Данные снова, вероятно, были почерпнуты из предыдущих нарушений.

«Я полагаю, что пары входа в систему появились из-за ранее сообщенных нарушений или сбора данных, поэтому они просто повторно используют их для учетных записей Spotify, чтобы стать частью этого автоматизированного процесса», - сказал Дьяченко.

В чем опасность заполнения учетных данных?

На первый взгляд, возможность киберпреступника войти в чью-то учетную запись Spotify может доставлять больше неудобств, чем что-либо еще. Создание мошеннических списков воспроизведения, удаление сохраненных песен или прямой захват возможности слушать музыку - вот некоторые из потенциальных головных болей.

Однако есть о чем подумать, отметил Дьяченко: для тех, кто повторно использует пароли, проверенная комбинация входа в систему Spotify может просто использоваться для проникновения в другие, более важные учетные записи.

«Технически, это не так опасно, если кто-то взломает вашу учетную запись Spotify (кроме моральной части, конечно)», - сказал он. «Однако в худшем случае ваши данные будут проданы подпольно или даже публично (я знаю, что для этого есть много реселлеров eBay)».

Взломанные учетные записи могут содержать информацию о кредитных картах, баллы лояльности, которые могут быть украдены или использованы, или физические адреса доставки. Кроме того, учетные записи могут содержать такую информацию, как дни рождения, предпочтения (например, плейлисты Spotify) и другие данные, которые могут быть использованы для злоупотреблений, когда речь идет о разработке приемов социальной инженерии для фишинговых атак.

Чтобы защитить себя от атак с заполнением учетных данных, пользователи должны включить многофакторную аутентификацию (MFA) для своих учетных записей и избегать использования паролей более одного раза». ***(Tara Seals. Spotify Suffers Second Credential-Stuffing Cyberattack in 3 Months // Threatpost (https://threatpost.com/spotify-credential-stuffing-cyberattack/163672/). 04.02.2021).***

***

«Компания «Яндекс» сообщает, что во время регулярной проверки ее служба безопасности выявила факт внутренней утечки данных.

Расследование показало, что один из сотрудников компании предоставлял несанкционированный доступ к почтовым ящикам пользователей. Это был один из трех системных администраторов, «обладавших такими правами доступа, необходимыми для выполнения рабочих задач по обеспечению технической поддержки сервиса». В результате его действий оказались скомпрометированы 4887 почтовых ящиков.

Сообщается, что в настоящее время неавторизованный доступ в скомпрометированные ящики уже заблокирован, а все пострадавшие получили уведомления о необходимости смены пароля. Также компания уже обратилась в правоохранительные органы.

«По выявленному инциденту проводится внутреннее расследование и будут пересмотрены процессы работы сотрудников, обладающих административными правами такого уровня доступа. Это поможет минимизировать влияние человеческого фактора на безопасность данных пользователей.

Мы очень сожалеем о случившемся и приносим извинения пользователям, которые пострадали из-за этого инцидента», — пишут представители «Яндекса». ***(Мария Нефёдова. В «Яндексе» обнаружили внутреннюю утечку данных // Xakep (https://xakep.ru/2021/02/12/ya-leak/). 12.02.2021).***

***

«Исследователи безопасности Талал Хадж Бакри (Talal Haj Bakry) и Томми Миск (Tommy Mysk) утверждают, что мобильные приложения Facebook Messenger и Instagram собирают и используют данные, доступные по передаваемым пользователями ссылкам, нарушая европейский закон о конфиденциальности (Директива 2002/58/ЕС).

Как обнаружили специалисты, мобильные версии программ Facebook Messenger и Instagram ведут себя не так, как другие приложения для обмена сообщениями, поскольку они загружают все содержимое любой ссылки на свои серверы, независимо от ее размера. Копии данных предварительного просмотра ссылок, хранящиеся на внешних серверах, могут быть похищены или неправомерно использованы, подвергая риску пользователей, которые отправляют ссылки на конфиденциальные или персональные данные, такие как деловые документы, счета, контракты или медицинские записи.

В декабре 2020 года компания Facebook объявила об изменениях в своих услугах в Европе, отключив определенные функции, не соответствующие закону о конфиденциальности. Хотя в Facebook не уточнили, какие именно функции были отключены, эксперты выяснили, что предварительный просмотр ссылок больше не доступен для пользователей в Европе. Это также касается пользователей за пределами данного региона, которые общаются с европейцами.

По словам исследователей, данные изменения являются неявным подтверждением того, что обработка Facebook предварительных просмотров ссылок в Messenger и Instagram не соответствовала европейским нормам конфиденциальности, поскольку в противном случаем техногигант не стал бы что-либо менять. Остановка работы данной службы в Европе явно намекает на то, что Facebook может использовать подобный контент для других целей, кроме создания превью.

Предварительный просмотр ссылок по-прежнему доступен в Messenger и Instagram для пользователей за пределами Европы. Текущие «Условия использования» Facebook гласят, что любой контент, которым пользователи делятся через любую из служб Facebook, будет использоваться для различных целей, таких как персонализация контента, реклама, внесение предложений и

изучение пользователей как в продуктах Facebook, так и за их пределами». ***(Facebook и Instagram заподозрены в нарушении закона о конфиденциальности ЕС // SecurityLab.ru (https://www.securitylab.ru/news/516428.php). 10.02.2021).***

***

«Американский телекоммуникационный провайдер T-Mobile раскрыл утечку данных после того, как неизвестное количество клиентов, очевидно, пострадали от атак с заменой SIM-карт.

Мошенничество с заменой SIM-карты (или угон SIM-карты) позволяет мошенникам получить контроль над телефонными номерами целей после переноса их с помощью социальной инженерии или после подкупа сотрудников мобильного оператора на SIM-карту, контролируемую мошенниками.

Впоследствии они получают сообщения и звонки жертв, что позволяет легко обойти многофакторную аутентификацию (MFA) на основе SMS, украсть учетные данные пользователей, а также захватить учетные записи онлайн-сервисов жертв.

Затем преступники могут войти в банковские счета жертв, чтобы украсть деньги, изменить пароли учетных записей и даже заблокировать доступ жертв к их собственным счетам.

ФБР поделилось рекомендациями о том, как защититься от подмены SIM-карт после увеличения числа атак с перехватом SIM-карт, нацеленных на приверженцев криптовалюты и инвесторов.

Неизвестное количество атак подмены SIM-карты

В уведомлении об утечке данных, отправленном пострадавшим клиентам 9 февраля 2021 года и поданном в офис генеральной прокуратуры США, T-Mobile сообщила, что неизвестный злоумышленник получил доступ к информации учетной записи клиентов, включая личную информацию и личные идентификационные номера (PIN-коды).

Поскольку злоумышленники смогли перенести номера, неясно, получили ли они доступ к учетной записи сотрудника или сделали это через учетные записи взломанных пользователей.

Представитель T-Mobile не был доступен для комментариев, когда сегодня с ним связались представители BleepingComputer.

«[A] Неизвестный субъект получил доступ к определенной информации учетной записи. Похоже, что субъект мог использовать эту информацию для переноса вашей линии на другого оператора без вашего разрешения», - сказал T-Mobile.

«T-Mobile идентифицировала эту деятельность - прекратила несанкционированный доступ и приняла меры для защиты от повторения».

Информация, к которой получили доступ хакеры, могла включать полные имена клиентов, адреса, адреса электронной почты, номера учетных записей, номера социального страхования (SSN), личные идентификационные номера учетных записей (PIN), вопросы и ответы по безопасности учетной записи, дату рождения, информацию о плане, и количество линий, на которые подписаны их аккаунты.

«T-Mobile быстро обнаружила и прекратила несанкционированные действия; однако мы рекомендуем вам изменить PIN-код вашей учетной записи», - заявили в компании.

Затронутым клиентам T-Mobile рекомендуется изменить пароль своей учетной записи, PIN-код, а также вопросы безопасности и ответы.

T-Mobile предлагает два года бесплатного кредитного мониторинга и услуг по обнаружению кражи личных данных через myTrueIdentity от Transunion.

Пятое нарушение данных за четыре года

Это пятая утечка данных, обнаруженная T-Mobile за последние четыре года, и все они были зарегистрированы после того, как хакеры получили доступ к данным клиентов.

Ранее T-Mobile страдала от взломов в 2018 году, когда хакеры получили доступ к информации о миллионах клиентов, а в 2019 году - после раскрытия данных предоплаченных клиентов…». ***(Sergiu Gatlan. T-Mobile discloses data breach after SIM swapping attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/t-mobile-discloses-data-breach-after-sim-swapping-attacks/). 26.02.2021).***

***

«Американская венчурная компания Sequoia Capital раскрыла утечку данных после того, что выглядело как неудачная атака с целью взлома деловой электронной почты (BEC) с января.

С момента своего основания в 1972 году венчурная компания Sequoia инвестировала в длинный список известных компаний (например, Apple, NVIDIA, Google, Oracle, Yahoo, LinkedIn, YouTube, Paypal, Electronic Arts и Cisco).

Гигант венчурного капитала также поддержал множество стартапов, включая Airbnb, Dropbox, FireEye, Palo Alto Networks, Stripe, Square и WhatsApp.

В целом компании, в которые Sequoia инвестировала на протяжении многих лет, теперь имеют «совокупную рыночную стоимость более 3,3 триллиона долларов».

Два месяца назад ФБР предупредило американские компании о том, что мошенники активно злоупотребляют правилами автоматической пересылки электронной почты, чтобы повысить успешность атак BEC.

Мошенники BEC используют сочетание социальной инженерии, фишинга и взлома для взлома корпоративных учетных записей электронной почты с конечной целью перенаправления платежей на банковские счета, находящиеся под их контролем.

Злоумышленники получили доступ к почтовому ящику сотрудника

«Примерно 20 января 2021 года мы узнали, что неавторизованная третья сторона получила удаленный доступ к служебному почтовому ящику электронной почты одного сотрудника Sequoia с очевидной целью проведения мошенничества с проводной версией», - поясняет Sequoia Capital в уведомлении о данных. нарушение отправлено пострадавшим лицам.

Хотя злоумышленники смогли взломать почтовый ящик сотрудника, они не получили доступа к другим ресурсам или активам в сети компании.

«Наше расследование не нашло никаких доказательств компрометации, кроме этого единственного почтового ящика», - сказал Секвойя.

Несмотря на то, что инцидент затронул единственный почтовый ящик, фирма ВК признала, что это могло позволить злоумышленникам извлечь личную информацию пострадавших.

«Несанкционированный доступ к почтовому ящику мог позволить третьей стороне получить копию файлов, включая личную информацию определенных лиц», - добавила Секвойя.

«В рамках нашего расследования мы проанализировали содержимое затронутого почтового ящика электронной почты и определили, что он содержит вашу личную информацию и что неавторизованная третья сторона могла получить доступ или получить ее копию».

Меры, принятые после нападения

После обнаружения атаки Sequoia Capital наняла внешних экспертов по безопасности для расследования инцидента и защиты своих систем.

Sequoia заявила, что не обнаружила никаких доказательств того, что киберпреступники продают или обменивают украденные данные в темной сети.

Компания также проинформировала соответствующие правоохранительные органы об атаке и приняла ряд мер в отношении аналогичных инцидентов в будущем, таких как:

Выявили и исправили конфигурацию, разрешившую первоначальный доступ;

Развернута дополнительная технология предотвращения и обнаружения на нескольких уровнях для улучшения видимости аномальной активности пользователей и вредоносного содержимого электронной почты;

Изучили методы, которые мы используем для хранения и обмена конфиденциальной информацией внутри и за пределами компании, включая правила пересылки сообщений электронной почты; и

Обновлены наши курсы по безопасности с дополнительным упором на осведомленность о фишинге и правильную обработку данных.

Sequoia предлагает пострадавшим лицам 24 месяца бесплатного кредитного мониторинга и защиту от кражи личных данных через Experian.

На выходных Axios сообщила о том, что венчурная компания информирует инвесторов о том, что ее взломали и что их информация могла быть скомпрометирована в результате утечки данных.

«Мы сожалеем о том, что этот инцидент произошел, и уведомили пострадавших лиц», - сказал представитель Sequoia Capital. «Мы вложили значительные средства в безопасность и продолжим делать это, работая над устранением постоянно развивающихся киберугроз». ***(Sergiu Gatlan. VC giant Sequoia Capital discloses data breach after failed BEC attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/vc-giant-sequoia-capital-discloses-data-breach-after-failed-bec-attack/). 25.02.2021).***

***

«Создание вредоносных макросов Office по-прежнему является наиболее распространенной техникой атаки, применяемой киберпреступниками, стремящимися взломать ПК после того, как они обманом заставили жертв открыть фишинговые электронные письма.

Фишинговые электронные письма являются первым этапом атаки для большинства кибер-вторжений, когда киберпреступники используют психологические приемы, чтобы убедить потенциальных жертв открыть вредоносные сообщения и взаимодействовать с ними.

Сюда может входить создание электронных писем, которые якобы исходят от известных брендов, поддельных счетов или даже сообщений, которые утверждают, что они исходят от вашего начальника.

Существует ряд методов, которые могут использовать киберпреступники, чтобы использовать фишинговые электронные письма для получения необходимого доступа, и, по мнению исследователей из компании Proofpoint, занимающейся кибербезопасностью, макросы Office являются наиболее распространенным средством достижения этой цели.

Макросы - это функция Microsoft Office, которая позволяет пользователям включать автоматические команды для выполнения задач. Однако киберпреступники злоупотребляют этой функцией. Поскольку макросы часто по умолчанию включены для выполнения команд, их можно использовать для выполнения вредоносного кода - и тем самым предоставить киберпреступникам скрытый способ получить контроль над ПК.

Во многих из этих кампаний будет использоваться социальная инженерия, чтобы побудить жертву включить макросы, заявив, что эта функция необходима для просмотра вложения Microsoft Word или Microsoft Excel. Это доказывает, что это успешный метод атаки для киберпреступников: на макросы Office приходится почти одна из 10 атак по объему.

Но макросы Office - далеко не единственная техника атаки, которую обычно используют киберпреступники, чтобы сделать хакерские кампании максимально успешными.

Уклонение от песочницы - второй наиболее распространенный метод атак, используемый преступниками, распространяющими фишинговые письма.

Это когда разработчики вредоносных программ встроили обнаружение угроз, которое останавливает запуск вредоносного ПО - эффективно скрывая его - если есть подозрение, что вредоносное ПО работает на виртуальной машине или воронке, созданной исследователями безопасности. Цель состоит в том, чтобы помешать аналитикам исследовать атаку и, следовательно, защитить от нее другие системы.

PowerShell также по-прежнему регулярно используется злоумышленниками как средство получения доступа к сетям после получения первоначальной плацдарма после фишингового письма. В отличие от атак с использованием макросов, они часто полагаются на отправку жертве, чтобы щелкнуть ссылку с кодом для выполнения PowerShell. Атаки часто трудно обнаружить, потому что

они используют законную функцию Windows, поэтому PowerShell остается популярным у злоумышленников.

Другие распространенные методы атаки, используемые для повышения эффективности фишинговых писем, включают перенаправление пользователей на веб-сайты, содержащие вредоносный HTML-код, который будет сбрасывать вредоносные программы на компьютер жертвы при их посещении, в то время как злоумышленники также известны тем, что просто захватывают потоки электронной почты, используя то, как жертвы будут доверять известный контакт и злоупотребление этим доверием в злонамеренных целях, например отправка вредоносного ПО или запрос учетных данных.

Данные о наиболее распространенных методах атак были получены из кампаний, нацеленных на клиентов Proofpoint, и анализа миллиардов электронных писем.

«Обучите пользователей обнаруживать вредоносную электронную почту и сообщать о ней. Регулярное обучение и имитация атак могут остановить многие атаки и помочь идентифицировать людей, которые особенно уязвимы. Лучшие симуляторы имитируют реальные методы атак», - заявили исследователи Proofpoint в своем блоге». ***(Danny Palmer. Phishing: These are the most common techniques used to attack your PC // ZDNet (https://www.zdnet.com/article/phishing-these-are-the-most-common-techniques-used-to-attack-your-pc/). 17.02.2021).***

***

«В то время как программы- вымогатели представляют собой кибератаки, которых больше всего опасаются компании, другая форма киберпреступности ускользает от радаров, которая оказывается очень прибыльной для интернет-мошенников и дорогостоящей для бизнеса.

Атака компрометации деловой электронной почты (BEC) заключается в том, что киберпреступники используют социальную инженерию, чтобы обманом заставить сотрудника компании перевести крупную сумму денег на счет, контролируемый мошенниками.

Часто эти сообщения якобы исходят от кого-то, кого жертва знает, например, от ее начальника, коллеги или другого известного и доверенного делового партнера. Злоумышленники могут украсть сотни тысяч долларов, просто отправив несколько электронных писем - и к тому времени, когда жертва поймет, что их обманули киберпреступники, уже слишком поздно.

И хотя программы-вымогатели являются наиболее распространенной формой киберпреступлений, нацеленных на бизнес, именно BEC-мошенничество наносит наибольший финансовый ущерб.

«Когда вы смотрите на некоторые из полученных данных, сравнивая компрометацию корпоративной электронной почты с такими вещами, как программы-вымогатели, компрометация деловой электронной почты, безусловно, составляет наибольшие финансовые потери для предприятий во всем мире», - Крейн Хассолд, старший директор по исследованию угроз. в Agari, рассказала серия видео ZDNet Security Update.

ФБР перечисляет BEC как киберпреступление с наибольшим объемом заявленных убытков, составив 1,77 миллиарда долларов только за 2019 год. Убытки от программ-вымогателей за тот же период составляют небольшую сумму по сравнению с 9 миллионами долларов (хотя более свежие цифры вымогателей будут значительно выше).

«Таким образом, хотя все новости узнают о программах-вымогателях, это ничто по сравнению с потерями, вызванными компрометацией корпоративной электронной почты», - сказал Хассолд.

Прибыльный характер мошенничества с BEC даже отталкивает некоторые киберпреступные операции от атак вредоносных программ и программ-вымогателей и в сторону мошенничества с использованием электронных переводов. Одна из них - российская хакерская группа, которую Агари идентифицирует как Cosmic Lynx - раньше они распространяли атаки вредоносного ПО, но теперь они зарабатывают гораздо больше денег на фишинге и мошенничестве с электронной почтой.

«За последние несколько лет мы увидели, что киберпреступники осознали, что их более технически сложные атаки стали менее успешными. Таким образом, киберпреступники стали менее технически изощренными в своих атаках». - сказал Хассольд.

«Если рассматривать это как бизнес с точки зрения накладных расходов, то за кулисами атаки BEC не так уж много, и поэтому сумма прибыли, которую вы можете получить от этих атак, значительно выше», - добавил он.

Одна из причин такого успеха BEC заключается в том, что природа ведения бизнеса в Интернете означает, что действия часто нужно предпринимать быстро - а поскольку больше людей работают удаленно, чем когда-либо прежде, проверить, действительно ли это электронное письмо пришло от вашего коллеги, сложнее.

Однако, если организация устанавливает бизнес-процессы, которым необходимо следовать, и требуется одобрение нескольких людей для отправки электронного перевода, это может иметь большое значение для предотвращения атак BEC.

«Если существует установленный процесс для телеграфного перевода и запросов на телеграфный перевод, то многие атаки BEC будут остановлены», - сказал Хассолд». ***(Danny Palmer. This cybersecurity threat costs business millions. And it's the one they often forget about // ZDNet (https://www.zdnet.com/article/this-cybersecurity-threat-costs-business-millions-and-its-the-one-they-often-forget-about/). 16.02.2021).***

***

«Киберпреступники постоянно адаптируют методы для распространения фишинговых писем, но простое раскрытие вашего адреса электронной почты или других личных данных в результате утечки данных повышает вероятность того, что вы станете мишенью в пять раз.

Google совместно со Стэнфордским университетом проанализировал более миллиарда фишинговых писем, которые киберпреступники пытались отправить пользователям Gmail в период с апреля по август прошлого года, и обнаружил, что

утечка личной информации в результате утечки сторонних данных после инцидента со взломом резко увеличивает вероятность стать мишенью для фишинговых писем по сравнению с пользователями, которые не опубликовали свои данные.

Другие факторы, которые могут повысить вероятность того, что вы подвергнетесь фишингу в соответствии с моделью Google, включают:

Также и там, где вы живете: в Австралии пользователи сталкиваются с вдвое большей вероятностью атаки по сравнению с США, хотя США являются самой популярной целью по объему (не на душу населения).

Шансы пережить приступ были в 1,64 раза выше для людей в возрасте от 55 до 64 лет по сравнению с людьми от 18 до 24 лет.

Пользователи, использующие только мобильные устройства, испытали меньшую вероятность атаки: 0,80 раза по сравнению с пользователями с несколькими устройствами. Google заявил, что это "может быть связано с социально-экономическими факторами, связанными с владением устройством и злоумышленниками, нацеленными на более состоятельные группы".

Google заявляет, что предотвращает попадание в почтовые ящики 99% из более чем ста миллионов электронных писем, содержащих спам, фишинговые ссылки и вредоносное ПО, которые ежедневно отправляются киберпреступникам, - но есть распространенные уловки, которые злоумышленники используют, чтобы обойти защиту.

Это предполагает использование быстро меняющихся кампаний, при этом определенные шаблоны писем рассылаются только в течение короткого периода времени. Иногда кампании могут длиться менее суток, прежде чем киберпреступники попытаются использовать другой шаблон для мошенничества по электронной почте.

Тем не менее, в исследовательском документе также отмечается, что фишинг - это постоянно развивающаяся область, и необходимы постоянные исследования, чтобы обеспечить максимальную защиту пользователей от атак.

«Наши измерения служат первым шагом на пути к пониманию того, как оценивать риски для личной безопасности. В конечном итоге такие оценки позволят автоматически определять, рекомендовать и адаптировать средства защиты для тех пользователей, которые в этом больше всего нуждаются», - говорится в документе.

В то время как пользователи, являющиеся мишенями фишинговых писем, обычно меняются от недели к неделе, характер атак остается в основном неизменным.

География также играет большую роль в том, попытаются ли киберпреступники совершить фишинговую атаку, при этом пользователи в США являются наиболее популярными целями, на которые приходится 42% атак. Далее следует Великобритания, на которую направлена каждая десятая фишинговая атака, и Япония, на которую направляется каждая 20-я фишинговая атака.

Хотя большинство злоумышленников не локализуют свои действия и используют английский язык в сообщениях, отправляемых в страны по всему миру, есть регионы, где электронные письма адаптированы для определенных языков.

Например, 78% атак, нацеленных на пользователей в Японии, произошли на японском языке, а 66% атак на пользователей из Бразилии произошли на португальском языке.

Google отмечает, что защита Gmail от фишинга и вредоносных программ включена по умолчанию, но также рекомендует пользователям использовать функцию проверки безопасности для получения персонализированных советов о том, как защитить свой почтовый ящик от фишинга и других вредоносных атак.

Корпоративным пользователям также рекомендуется развернуть расширенную защиту от фишинга и вредоносного ПО от Google». ***(Danny Palmer. Google: Here's why some people get more phishing emails and malware spam // ZDNet (https://www.zdnet.com/article/google-heres-why-some-people-get-more-phishing-emails-and-malware-spam/). 10.02.2021).***

***

«За последний год резко увеличилось количество киберпреступников, пытающихся провести атаки с использованием учетных данных удаленного входа, поскольку многие сотрудники продолжают работать из дома.

Для многих работа из дома стала необходимостью, и только удаленный вход в корпоративные сети VPN и наборы приложений позволяет людям продолжать выполнять свою работу.

Однако рост удаленной работы предоставил киберпреступникам больше возможностей незаметно проскользнуть в сети с помощью законных учетных данных - независимо от того, были ли они фишинговыми, угаданными или украденными иным образом. Используя законные данные для входа в систему вместо развертывания вредоносного ПО, злоумышленникам легче заниматься своими делами, не будучи обнаруженными.

По данным исследователей из компании ESET, занимающейся кибербезопасностью, такая легкость привела к увеличению числа атак по протоколу удаленного рабочего стола (RDP) на 768% в течение 2020 года. В общей сложности ESET обнаружила 29 миллиардов попыток RDP-атак за год, поскольку киберпреступники пытаются использовать удаленных сотрудников.

В некоторых случаях порты RDP даже неправильно настроены, что дает злоумышленникам еще больший доступ к сетям.

В любом случае, атаки RDP могут использоваться для проникновения в сеть с целью изучения и кражи конфиденциальной информации, а также как средство получения достаточного доступа к сети для развертывания атак программ-вымогателей.

Это все в средах, которые могут быть менее защищены, чем если бы сотрудники работали изнутри офиса, а не работали удаленно.

«Атаки RDP сосредоточены на технологиях, а не на людях, поэтому от злоумышленников требуется меньше ручной работы. Неверно настроенный RDP во многих случаях приводит к использованию ценных ресурсов, таких как серверы компании или устройства с правами администратора, которые представляют собой трамплин для дальнейшего, часто сетевого - в целом, компромиссы», - сказал ZDNet Ондрей Кубович, специалист по безопасности в ESET.

В отчете ESET отмечается, что в декабре количество атак RDP снизилось, что они приписывают киберпреступникам, которые взяли отпуск на Рождество. Но ожидается, что в 2021 году киберпреступники по-прежнему будут пытаться использовать атаки RDP для проникновения в корпоративные сети, особенно если сотрудники продолжают работать удаленно.

Однако существуют действия, которые организации могут предпринять, чтобы киберпреступникам было намного сложнее успешно взломать сеть с помощью RDP-атак.

SEE: жертвы программ-вымогателей не сообщают об атаках в полицию. Это вызывает большую проблему

Команды ИТ-безопасности должны поощрять пользователей использовать надежные пароли, которые трудно угадать при атаках методом грубой силы. Этот пароль не следует использовать для каких-либо других учетных записей, чтобы снизить риск взлома в результате утечки или взлома пароля в другом месте.

Применение двухфакторной аутентификации в сети также будет иметь большое значение для предотвращения успешных атак RDP киберпреступниками, поскольку намного сложнее получить дополнительный уровень проверки, необходимый для доступа к учетным записям.

Обеспечение использования пользователями последних версий операционных систем и программного обеспечения за счет наличия надежной стратегии установки исправлений также может обеспечить дополнительный уровень защиты от попыток атак». ***(Danny Palmer. Big jump in RDP attacks as hackers target staff working from home // ZDNet (https://www.zdnet.com/article/big-jump-in-rdp-attacks-as-hackers-target-staff-working-from-home/). 08.02.2021).***

***

«Компания веб-хостинга под названием No Support Linux Hosting объявила сегодня о закрытии после того, как хакер взломал ее внутренние системы и поставил под угрозу всю ее работу.

Согласно сообщению, размещенному на официальном сайте [в архиве], компания заявила, что взлом была взломана в понедельник, 8 февраля. Похоже, что хакер «скомпрометировал» всю деятельность компании, включая ее официальный веб-сайт, раздел администратора и базу данных клиентов.

Представитель No Support Linux Hosting (NSLH) не ответил на запрос о комментариях с подробностями об атаке. Но хотя подробности о вторжении неясны, атака, похоже, имела разрушительный характер.

«Мы больше не можем вести бизнес без поддержки Linux Hosting», - категорически заявила сегодня компания.

«Все клиенты должны немедленно загрузить резервные копии своих веб-сайтов и баз данных через cPanel», - сказал NSLH, призвав клиентов сделать это до того, как серверы выйдут из строя навсегда.

На момент написания статьи природа NSLH-атаки неясна, и мы не знаем, загрузил ли хакер и стер базу данных и резервные копии компании или мы говорим о классической атаке вымогателей, когда злоумышленник зашифровал файлы и потребовал выкуп за ключ дешифрования.

ДВА ДРУГИХ ХОСТИНГ-ПРОВАЙДЕРА ТАКЖЕ СООБЩИЛИ О ВЗЛОМАХ

Но даже если NSLH не ответила на запрос о комментарии, похоже, что в этой атаке есть намного больше.

Ранее сегодня TorrentFreak, блог, посвященный цифровым правам и новостям о пиратстве, сообщил, что две британские хостинговые компании, которые предоставляют услуги IPTV пиратским потоковым сайтам, также пострадали от аналогичных атак.

На короткое время в понедельник SapphireSecure.net и KS-Hosting.com показали на своей первой странице сообщение от предполагаемого хакера.

В сообщении хакер поделился личными данными человека, стоящего за двумя сайтами, и пригрозил двум компаниям поделиться своими клиентскими базами данных с полицией и агентствами по защите авторских прав, если не будет уплачен выкуп в размере 2 BTC (~ 92 000 долларов США).

Но что может связать эту атаку с инцидентом NSLH, так это тот факт, что хакер SapphireSecure.net и KS-Hosting.com также дал компаниям возможность навсегда прекратить работу, чтобы избежать передачи их данных властям или уплаты выкупа.

Поскольку два взлома находятся так близко друг к другу и имеют частично совпадающие детали, возможно, что NSLH был взломан одним и тем же злоумышленником». ***(Catalin Cimpanu. Web hosting provider shuts down after cyberattack // ZDNet (https://www.zdnet.com/article/web-hosting-provider-shuts-down-after-cyber-attack/). 09.02.2021).***

***

«Французское Национальное агентство безопасности информации (ANSSI), национальное агентство по кибербезопасности, определило многолетнюю кампанию по проникновению на платформу мониторинга ИТ Centreon.

Centreon (компания) заявила, что Centreon (программное обеспечение) - это отличный инструмент для мониторинга ИТ с открытым исходным кодом.

«Организации должны пристально следить за своей ИТ-инфраструктурой и операциями, чтобы гарантировать время безотказной работы и максимальную доступность сети», - говорится в рекламном сообщении компании. Компания Centreon заявила, что программное обеспечение Centreon - это тот немигающий глаз.

Анси в понедельник показал, что известно о двух бэкдоров в Centreon на программное обеспечение и сказал провайдеры несколько французских ИТ услуги были проникали на срок до трех лет.

В подробном отчете [PDF] о том, что The Register использовала заржавевшие французские службы средней школы и онлайн-переводчики, ANSSI сообщает, что атака использовала веб-оболочку PAS и троян-бэкдор Exaramel.

Ни один бэкдор не является новым. Веб-оболочка PAS находится на радарах поставщиков средств безопасности с 2017 года, а упоминания об Exaramel можно найти в 2018 году. PAS делает неприятные вещи, включая атаки грубой силы на

базы данных, чтобы получить доступ к их содержимому. Exaramel - это инструмент дистанционного управления.

ANSSI заявило, что атака возможна, потому что некоторые пользователи Centreon не установили исправления для своих систем. Агентство не описало последствий атаки, но заявило, что комбинация двух бэкдоров позволила полностью скомпрометировать Centreon, программное обеспечение и, следовательно, горизонтальное перемещение по сетям.

Поскольку атака была нацелена на поставщиков услуг, и такие организации, вероятно, будут предлагать многопользовательскую инфраструктуру, возможно, многие объекты были скомпрометированы.

ANSSI не сказал, что Россия несет ответственность за атаку, но сказал, что методы, использованные для установки бэкдоров и управления ими, очень похожи на команду «Sandworm», которая также подозревается в причастности к программе-вымогателю NotPetya.

В отчете ANSSI рекомендуется, чтобы все пользователи инструментов управления ограничили доступ к своим веб-интерфейсам и укрепили серверы Linux, на которых они работают.

Но поставщикам ИТ-услуг и поставщикам, которые удовлетворяют их потребности, постоянно напоминают, что высокий уровень безопасности не подлежит обсуждению, потому что они являются воротами для множества других организаций и, следовательно, являются основной целью для преступников. Тем не менее, некоторые явно использовали старые и уязвимые версии программного обеспечения Centreon, а затем не смогли обнаружить злоумышленников, роющихся внутри.

Как и многие организации, которые использовали скомпрометированные версии программного обеспечения для управления Orion от SolarWinds». ***(Simon Sharwood. France's cyber-agency says Centreon IT management software sabotaged by Russian Sandworm // The Register (https://www.theregister.com/2021/02/16/centreon_sandworm_attack/). 16.02.2021).***

***

«Эксперты ООН пришли к выводу, что КНДР обновила собственный ракетный и ядерный потенциал на деньги, полученные в результате кибератак на криптобиржи и финансовые интернет-сервисы. Украденные активы после «отмывания» в Китае расходуются на закупки материалов и технологий.

Бомба сама себя не сделает

Корейская народно-демократическая республика (КНДР) в обход санкций Организации объединенных наций (ООН) модернизировала свое ядерное оружие за счет средств, украденных, в том числе, правительственными хакерами. Такие выводы изложены в новом отчете группы экспертов, направленном членам Совета безопасности ООН.

По мнению экспертов, связанные с Северной Кореей злоумышленники на протяжении всего 2020 г. продолжали проводить кибератаки на финансовые учреждения и виртуальные обменные пункты. Украденные таким образом

финансовые активы, в том числе криптовалюта, направлялись на поддержку правительственных программ КНДР в области совершенствования оружия массового уничтожения и баллистических ракет, а также на приобретение соответствующих материалов и технологий за рубежом.

Криптовалютные активы, украденные северокорейскими хакерами, проходят процесс «отмывки» через китайских внебиржевых брокеров и затем конвертируются в фиатные (обеспеченные государством) валюты, например, в доллар США, сообщило агентство Associated Press со ссылкой на доклад экспертов ООН.

Так, только в период с 2019 г. по ноябрь 2020 г., по данным экспертов, суммарный ущерб от северокорейских кибератак составил примерно $316,4 млн. В августе 2019 г. комиссия ООН также обвинила северокорейских киберпреступников в незаконном получении доходов на сумму порядка $2 млрд, которые также были направлены на финансирование госпрограмм по разработке оружия.

Взлом по-северокорейски

В своем отчете эксперты ООН представили расследование «умышленно вредительской» деятельности Главного разведывательного бюро (Reconnaissance General Bureau) Северной Кореи, которое уже находится в санкционном списке ООН, в частности, за атаки на виртуальные активы, на поставщиков виртуальных финансовых услуг и на оборонные компании.

В качестве примера эксперты ООН привели случай взлома криптовалютной биржи в сентябре 2020 г. когда была украдена криптовалюта на сумму порядка $281 млн. Связанные с этим эпизодом блокчейн-транзакции также показали связь взлома на $281 млн со вторым взломом на $23 млн в октябре 2020 г.

По мнению экспертов, предварительный анализ этих событий, основанный на векторах атак и последующих действиях по отмыванию незаконных доходов, убедительно свидетельствует о связях с КНДР.

Еще одним способом добычи незаконных доходов северокорейскими кибермошенниками, по словам экспертов, также является использование ИТ-платформ для фрилансеров, где используются те же методы, что и для доступа к мировой финансовой системе – фальшивая идентификация, сервисы VPN и подставные компании в Гонконге.

В августе 2020 г. CNews рассказал о действиях северокорейской кибергруппировки Lazarus, которая переключилась с традиционных финансовых учреждений на криптобиржи. Механизм взлома включает рассылку сисадминам криптобирж фальшивых предложений о работе через Linkedin с вредоносным документом Word.

Самоизоляция в эпоху глобальной изоляции

Совет безопасности ООН последовательно проводит политику ужесточения экономических санкции против Северной Кореи, начиная с первого испытательного взрыва ядерного устройства в стране, проведенного, как писал CNews, в 2006 г. Пытаясь заставить Пхеньян отказаться от программ по созданию ядерного оружия и баллистических ракет, ООН ввела запрет на большую часть экспорта и импорта страны.

Ядерный арсенал КНДР превратился в серьезную угрозу после испытаний в 2017 г., когда власти страны объявили о подрыве термоядерной боеголовки и летных испытаниях межконтинентальных баллистических ракет, которые теоретически могут достигать континентальной части территории США.

Наследный руководитель КНДР Ким Чен Ын (Kim Jong Un) ранее уже объявил о проведенной модернизации инфраструктуры баллистических ракет, разработке тактического ядерного оружия и подготовке к испытаниям и производству боеголовок баллистических ракет нового типа, отмечают эксперты.

На последних военных парадах руководство страны продемонстрировало новые системы баллистических ракет малой и средней дальности и для подводных лодок, а также межконтинентальных баллистических ракет. Кроме того, у экспертов ООН имеется информация о налаженном в КНДР производстве расщепляющихся материалов для ядерного оружия.

В 2020 г. плохое состояние экономики Северной Кореи еще более ухудшилось из-за пандемии COVID-19. Ким Чен Ын был вынужден закрыть границы страны, что максимально ограничило перемещение товаров и людей – как законных, так и незаконных.

В январе 2021 г. на съезде правящей Рабочей партии Ким Чен Ын призвал к усилению госконтроля над экономикой и пообещал продолжить всестороннее развитие ядерной программы. Позже, в рамках политической конференции он также обрушился с резкой критикой на экономическое крыло своего правительства за пассивность.

В 2018 г. Ким Чен Ын начал дипломатические переговоры с Южной Кореей и США, однако Дональд Трамп (Donald Trump), занимавший в то время должность президента США, отклонил в 2019 г. требования Северной Кореи о значительном ослаблении санкций в обмен на частичное сокращение ядерного арсенала КНДР.

Нынешний президент США Джо Байден (Joe Biden) ранее называл Ким Чен Ына «головорезом» (Thug) и последовательно критиковал Трампа за «саммиты-спектакли» на высшем уровне вместо реальных усилий по сокращению ядерных вооружений КНДР». ***(Владимир Бахур. Северная Корея резко нарастила ядерный потенциал на деньги, украденные ее хакерами // CNews (https://safe.cnews.ru/news/top/2021-02-09_severnaya_koreya_tratit_kradennuyu). 09.02.2021).***

***

«Некоторые эксперты по кибербезопасности соглашаются с отчетом Cybersecurity Ventures и ожидают, что к концу этого года финансовый ущерб от киберпреступности достигнет 6 триллионов долларов. Отраслевые исследования показывают, что кибератаки являются одними из самых быстрорастущих преступлений в США.

Количество кибератак постоянно растет. По словам Роберта Маккея, старшего вице-президента компании Neustar по решениям для управления рисками, на основе всего, что мы знаем, и каждого аналитика, с которым мы разговаривали, количество атак возрастает.

«Эксперты по кибербезопасности прогнозируют, что в 2021 году кибератаки будут происходить каждые 11 секунд. Это почти вдвое больше, чем было в 2019 году (каждые 19 секунд), и в четыре раза больше, чем пять лет назад (каждые 40 секунд в 2016 году)», - сказал он. сообщил TechNewsWorld.

Быстро растущий рост кибератак во всем мире дорого обходится компаниям, которые стремятся лучше защитить свои компьютерные сети от вторжений. Кибератаки не только учащаются, но и приносят жертвам большие финансовые потери.

Растущая цена киберриска

Согласно данным, проанализированным исследователями Atlas VPN, во всем мире киберпреступность обходится предприятиям, правительственным учреждениям и потребителям в целом более чем в 1 триллион долларов в 2020 году. Это около одного процента мирового ВВП.

В то время как 945 миллиардов долларов было потеряно из-за киберинцидентов, 145 миллиардов долларов было потрачено на кибербезопасность. Эти затраты увеличились более чем на 50 процентов по сравнению с 2018 годом, когда на борьбу с киберпреступностью было потрачено более 600 миллиардов долларов.

Но, согласно отчету Atlas VPN, двадцать процентов организаций во всем мире не имеют планов по защите от киберпреступлений. Это оставляет зияющую дыру в сетях, позволяющую киберпреступникам расширить свои стратегии атак, чтобы украсть еще миллионы долларов.

Единственная надежная защита, предупреждают эксперты по кибербезопасности, - это активизировать усилия по принятию законодательства, которое укрепляет технологическую защиту. Возможно, это единственный способ изменить ход продолжающихся кибератак.

Несмотря на все усилия по защите систем и данных, взломы облачных вычислений, вероятно, будут увеличиваться как по скорости, так и по масштабу, сказал Джон Кинселла, главный архитектор Accurics, о летнем исследовательском отчете его компании о состоянии DevSecOps в 2020 году.

«Этот [анализ] проводится по мере того, как в последние два года наблюдается свирепое распространение облачных атак. В результате неправильной конфигурации облачной инфраструктуры обнаружено более 30 миллиардов записей», - сказал он TechNewsWorld.

Он добавил, что для того, чтобы идти в ногу с развивающейся экономикой, которая требует большей цифровой трансформации, организации должны поставить киберустойчивость и практику DevSecOps во главу своих приоритетов.

Не только в облаках

Рост кибератак приводит к гораздо большему успеху, чем безудержная миграция в облачное хранилище и неверно настроенная облачная инфраструктура. Тем не менее, неправильная конфигурация в облачной инфраструктуре приводит к раскрытию данных и является одной из самых серьезных киберугроз, с которыми сегодня сталкиваются бизнес и государственные учреждения, - отметил Кинселла.

Почти 98 процентов всех кибератак основываются на той или иной форме социальной инженерии для доставки полезной нагрузки, такой как вредоносное ПО

или программы-вымогатели. Один из наиболее успешных форматов атак, которые киберпреступники регулярно используют для проведения атак социальной инженерии, - это фишинговые электронные письма. Таким образом, злоумышленники распространяют вредоносное ПО по электронной почте примерно в 92 процентах случаев.

Использование облака и постоянное распространение облачных сервисов никуда не денутся. Этим продолжающимся сдвигом в вычислительной практике необходимо управлять с большей бдительностью.

COVID ускорил цифровую трансформацию организаций. Следовательно, возможность создавать рабочие нагрузки в облаке и решать проблемы соответствия и безопасности является востребованной, - отметил Мохит Тивари, соучредитель и генеральный директор Symmetry Systems.

«Отчасти причина в том, что рабочие нагрузки, которые сопротивлялись переходу в облако, были строго регулируемыми, а вынужденный уход из локальных центров обработки данных, управляемых ИТ-персоналом, повышает спрос на облачные навыки соответствия и безопасности.», - сказал он TechNewsWorld.

Таким образом, облачные методы безопасности будут иметь жизненно важное значение в борьбе с ухудшающимся ландшафтом кибербезопасности. К ним относятся обучение работе с облачной идентификацией и управлением доступом (IAM), отметил он.

«Тем, кто заботится о облачной безопасности, необходимо в целом научиться управлять инфраструктурой с помощью структурированных программ, а не сценариев оболочки, собранных вместе. По мере того, как сети и уровни приложений становятся эфемерными, наиболее важным постоянным активом для любого предприятия, вероятно, будут они сами и их клиенты «Таким образом, безопасность данных в облаке будет главной темой в будущем», - предупредил он.

Обеспечение облачного покрова

Мировая пандемия ускорила кибер-вторжения. Так же, как и самоуспокоенность, плохая подготовка офисных работников и неадекватное наблюдение за ИТ.

Организации должны рассмотреть сбалансированный подход к обучению своих сотрудников и инвестированию средств в средства автоматизации, чтобы минимизировать риски кибератак, - предложил Брендан О'Коннор, генеральный директор и соучредитель AppOmni. Нет необходимости в обширном обучении и круглосуточном ручном мониторинге, если правильные инструменты автоматизации могут дополнять ИТ-персонал по мере его повышения.

«ИТ-специалистам, специализирующимся на безопасности, необходимо переключить свое внимание на поддержку новой модели бизнеса, которую внедряют многие предприятия. Некоторые предприятия меняют свою бизнес-модель, чтобы сосредоточиться на виртуальной рабочей силе, не обращая внимания на необходимость защиты офисных сетей», - О'Коннор сообщил TechNewsWorld.

В других случаях офисы ликвидируют совсем. Он продолжил, что ИТ-специалистам необходимо сменить фокус с традиционной сетевой безопасности кампуса / офиса на безопасность приложений модели «работа в любом месте».

«Поскольку местонахождение сотрудников и устройства постоянно меняются, организации будут полагаться на согласованность и безопасность приложений облачных сервисов. ИТ-работникам следует рассматривать управление и безопасность этих приложений SaaS (программное обеспечение как услуга) как новые навыки и технологии, которые следует использовать, "Сказал О'Коннор.

Надвигающиеся угрозы

В течение следующего года программы-вымогатели будут оставаться самой большой угрозой и финансовым риском для предприятий, заметил Джозеф Карсон, главный специалист по безопасности и консультант по информационной безопасности компании Thycotic. Он посоветовал большинству организаций быть очень обеспокоены программами-вымогателями как самой большой проблемой и угрозой кибербезопасности.

«Организации должны уделять первоочередное внимание инвестициям в решения безопасности, которые помогают снизить риски, а также планировать и тестировать план реагирования на инциденты, чтобы гарантировать устойчивость бизнеса к атакам с высоким риском», - сказал он TechNewsWorld.

Программа-вымогатель продолжает превращаться в нечто большее, чем просто нарушение безопасности. Киберпреступники теперь ищут утечки данных с организованными группами киберпреступников, чтобы украсть данные, прежде чем они будут зашифрованы на корпоративных серверах. Компании беспокоятся не только о том, чтобы вернуть свои данные, но и о том, кому они будут предоставлены публично.

По словам Карсона, киберпреступники используют программы-вымогатели, чтобы атаковать кого угодно, любую компанию и любое правительство, включая больницы и транспортную отрасль, в то время, когда они находятся под сильным давлением.

Еще одна серьезная тенденция атак кибербезопасности сосредоточена на средствах защиты и поставщиках средств безопасности в отрасли, - отметил Брэндон Хоффман, директор по информационной безопасности в Netenrich. Инструменты, на которые полагается отрасль, и их поставщики становятся все более целями атак.

«Это серьезная проблема, потому что практикам нужны инструменты, на которые они могут положиться для обнаружения и защиты. Подавляя или перепрофилируя те самые инструменты, которые предназначены для предотвращения этих попыток, злоумышленники могут получить полное преимущество в продолжающейся битве по борьбе с киберугрозами, "Хоффман сказал TechNewsWorld.

«Атаки, нацеленные на организации и поставщиков, занимающихся безопасностью, всегда занимали первое место в списке противников, но успех порождает дальнейший успех».

Борьба с битвой

Фактор доверия - это своего рода внутренняя битва между поставщиками средств безопасности и корпорациями, нанимающими их для киберзащиты. «Это

доверие необходимо постоянно пересматривать», - предложил Тим Уэйд, технический директор группы технического директора Vectra AI.

«В стратегическом плане специалисты по безопасности должны продолжать переходить от превентивной архитектуры безопасности к архитектуре безопасности, основанной на устойчивости», - сказал Уэйд TechNewsWorld.

Именно здесь акцент смещается на признание реальности того, что что-то пойдет не так, но когда это произойдет, влияние сведено к минимуму за счет быстрого обнаружения, реагирования и восстановления, добавил он. Продавцы и поставщики всегда были прибыльной целью для злоумышленников.

Многие кибератаки принадлежат к организованным преступным группировкам, подпадающим под санкции иностранных государств. Лучшая защита таких противников - это признание того, что вы не можете их остановить. Но затем сосредоточьтесь на том, чтобы сделать их жизнь как можно более сложной, - сказал Уэйд.

Кибербезопасность Высшее образование

Одним из часто негласных способов защиты от атак кибербезопасности является образование. Этот подход выходит за рамки обучения сотрудников компании лучшему пониманию идеалов безопасных вычислений. Скорее, найм следующего поколения компьютерных специалистов для получения степени в области кибербезопасности.

Кибербезопасность процветает, потому что так много профессионалов имеют разный опыт и навыки, отметила Хизер Паунет, старший вице-президент Untangle.

«Группы, которые традиционно маргинализируются в других отраслях, когда начинают карьеру в области кибербезопасности или начинают карьеру в сфере кибербезопасности, могут получить выгоду от нескольких ведущих организаций, предлагающих программы сертификации», - сказала она TechNewsWorld.

«Развивающаяся сфера кибербезопасности - очень жизнеспособный карьерный путь», - отметил Майкл Качмарек, вице-президент по управлению продуктами Neustar. Отраслевые отчеты показывают, что количество незаполненных вакансий в сфере кибербезопасности вырастет на 35 процентов.

«Учитывая рост атак и изменение тактики, используемой злоумышленниками и организациями, кибербезопасность, безусловно, станет выбором карьеры, который обеспечит чистую занятость в долгосрочной перспективе», - сказал он TechNewsWorld.

Спрос на вакансии в сфере кибербезопасности, безусловно, увеличился за последний год, согласен Дов Лернер, руководитель исследований в области безопасности в Sixgill. Карьерный путь в этой сфере - отличный выбор для тех, кто интересуется ИТ и безопасностью.

«Увеличение количества используемых инструментов увеличивает сложность операций по обеспечению безопасности и аналитики и требует увеличения персонала. Однако, согласно недавнему опросу ESG, почти 70 процентов групп безопасности говорят, что трудно нанять и нанять дополнительных SOC (операций безопасности center)», - сказал Лернер TechNewsWorld.

Аналитики безопасности имеют возможность повлиять не только на свою отрасль. Кибербезопасность проникает в мир политики, экономики и других секторов мира. «Пробиться на поле боя может быть непросто, но это невероятно полезно», - заключил он». ***(Jack M. Germain. The Future of Cybersecurity in 2021 and Beyond // ECT News Network (https://www.technewsworld.com/story/The-Future-of-Cybersecurity-in-2021-and-Beyond-87018.html). 16.02.2021).***

***

«Канадский исследовательский университет для студентов Лейкхед столкнулся с кибератакой, которая вынудила учреждение в начале этой недели перекрыть доступ к своим серверам.

Службы школы, в том числе ее веб-сайт, были отключены со вторника, сотрудники отключили компьютеры в кампусах Тандер-Бей и Ориллии, чтобы предотвратить распространение атаки.

Услуги по-прежнему не работают

В сообщении в четверг университет Лейкхед предоставил некоторые подробности об атаке, заявив, что она была нацелена на его серверы общего доступа к файлам. Однако в школе не раскрывают природу происшествия.

«Как только Центр технологических услуг Lakehead (TSC) узнал о потенциальной угрозе для наших серверов, TSC полностью закрыл к ним доступ», - заявили в университете.

В настоящее время проводится расследование, пытаясь определить, какие серверы и информация были затронуты инцидентом безопасности. Пока оценка не будет завершена, «вся информация, используемая и хранимая на наших общих файловых серверах, будет недоступна, а компьютеры в кампусе не будут доступны для использования».

Университет рекомендует всем, кто хранит учетные данные в документах в своей системе обмена файлами или на офисном компьютере университетского городка, изменить свои пароли в качестве меры предосторожности.

Хотя это разумная рекомендация в случае взлома, тот факт, что атака распространилась на офисные компьютеры кампуса, может указывать на атаку программы-вымогателя. Однако, как упоминалось ранее, университет не раскрыл ни характера атаки, ни ее масштабов.

На данный момент официальные лица школы не сообщили, затронула ли атака личную или финансовую информацию, обрабатываемую университетом.

Затронута успеваемость

Университет Лейкхед отменил все свои мероприятия, в том числе вебинары и виртуальные туры по кампусу Тандер-Бей и Ориллии, запланированные на эту пятницу.

Из-за того, что все службы не работают, некоторые студенты не могут общаться со своими инструкторами, получать академический календарь, пользоваться библиотекой, подавать документы или платежи в установленный срок.

В пятницу в твите Лейкхедский университет предложил студентам, преподавателям и сотрудникам возможное решение для доступа к электронной

почте. Однако этот метод работает не во всех случаях. В школе заявили, что если в браузере доступна информация для входа в систему, пользователи могут загружать почтовый ящик Gmail.

Учащиеся полагаются на услуги школы для доступа к платформам онлайн-обучения. Ссылки на курсы, сервисы Google (Gmail, Docs) и университетская библиотека необходимы им для подготовки к промежуточным экзаменам.

На данный момент руководство университета не приняло решения о переносе сроков выполнения заданий, переносе экзаменов или продлении недели чтения, несмотря на ходатайство студентов, но не исключает этого. Они намерены в ближайшее время восстановить услуги и начать занятия в понедельник». ***(Ionut Ilascu. Lakehead University shuts down campus network after cyberattack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/lakehead-university-shuts-down-campus-network-after-cyberattack/). 21.02.2021).***

***

«Группа вредоносной рекламы ScamClub использовала уязвимость нулевого дня в движке веб-браузера WebKit для отправки полезных данных, которые перенаправлялись на мошенничество с подарочными картами.

Во время их кампаний за последние три месяца количество показов злонамеренной рекламы за день достигло 16 миллионов.

Злоумышленники ScamClub печально известны своей шумной тактикой, заключающейся в наводнении рекламной экосистемы вредоносной рекламой в надежде, что через нее пройдет меньший процент.

Даже если большая часть рекламы заблокирована, ее объем настолько велик, что необнаруженные объявления приводят к значительному количеству злонамеренных показов в течение одной кампании.

Описывая «стратегию бомбардировки» ScamClub, компания Confiant, занимающаяся безопасностью рекламы и контролем качества, говорит, что улучшение коэффициента перенаправления всего на 1% может привести к «десяткам тысяч затронутых показов» в течение одной кампании.

Лазейка

Наблюдая за деятельностью ScamClub, в июне 2020 года Confiant заметил в запутанном коде полезной нагрузки четыре строки со слушателем событий, что вызвало любопытство исследователей.

В блоге пос т сегодня, Confiant инженер безопасности и исследователь Элия Штейн обнаружил, что malvertiser полагались на уязвимости в WebKit, который обходил Песочница политику IFrame.

Продолжая расследование, исследователь удалил ненужный код и подготовил простой HTML-файл с изолированным фреймом из разных источников и кнопкой, которая отправила событие, при этом полезная нагрузка была слушателем.

Стейн отмечает, что атрибут песочницы «allow-top-navigation-by-user-activate» в приведенном выше доказательстве кода концепции должен предотвращать любое перенаправление. Это действительно, если не происходит правильной активации, что в данном случае означает щелчок внутри рамки.

«Это означает, что наше доказательство концепции не должно работать ни при каких обстоятельствах. В конце концов, кнопка clickMe находится за пределами изолированного фрейма. Однако, если она выполняет перенаправление, это означает, что у нас в руках ошибка безопасности браузера, которая оказалась будет в случае тестирования в браузерах на основе WebKit, а именно в Safari для ПК и iOS», - Элия Стейн

Хотя теоретически это должно предотвратить злонамеренные перенаправления, исследователь далее объясняет, что сообщения с подстановочными знаками назначения в современных веб-приложениях являются обычным явлением и часто возникают при взаимодействии с пользователем.

Учитывая широкий таргетинг SscamClub и большие объемы вредоносной рекламы, которую они размещают, некоторые из них все же проскальзывают и оказывают значительное влияние. Ниже приведены домены, используемые в рекламных кампаниях ScamClub.

Для сравнения: Confiant приписывает группе ScamClub более 50 миллионов вредоносных показов за последние 90 дней, причем пики затронутой рекламы достигли 16 миллионов в день.

Поскольку WebKit используется в Chrome на iOS и Safari, Штайн представил свои выводы как в Apple Security, так и в команду Google Chrome. 2 декабря 2020 года WebKit получил патч, и уязвимости был присвоен идентификатор CVE-2021-1801.

Confiant выпустила индикаторы компрометации (IoC) в своем репозитории GitHub, которые включают размещение полезных нагрузок в облаке Amazon и домены, используемые в недавних кампаниях ScamClub». ***(Ionut Ilascu. Malvertisers exploited browser zero-day to redirect users to scams // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/malvertisers-exploited-browser-zero-day-to-redirect-users-to-scams/). 16.02.2021).***

***

«2020 год был неудачным для медицинских организаций в США, которым пришлось столкнуться с рекордным количеством инцидентов в области кибербезопасности на фоне пандемии COVID-19.

Хакерские атаки и ИТ-инциденты в большей степени повлияли на отрасль в прошлом году, составив более 67% всех взломов и раскрывая личные данные десятков миллионов людей.

Наибольшее количество нарушений

Анализ данных от Министерства здравоохранения и социальных служб США, компании по защите от угроз.

Bitglass обнаружила, что количество нарушений в сфере здравоохранения, зарегистрированных в 2020 году, увеличилось до 599, что более чем на 50% по сравнению с предыдущим годом (386).

Большинство нарушений было вызвано хакерскими атаками и ИТ-инцидентами, в результате которых были раскрыты данные 24,1 миллиона человек, что сделало их уязвимыми для кражи личных данных и фишинговых атак.

Однако, несмотря на рост числа инцидентов, общее количество пострадавших несколько ниже по сравнению с 2019 годом.

Разбивка нарушений по штатам показывает, что наибольшее количество инцидентов было в Калифорнии, 49 инцидентов, за ней следует Техас с 43.

Следующие три позиции занимают Нью-Йорк с 39 нарушениями, Флорида и Пенсильвания, каждая с 38 нарушениями.

Если посмотреть на штаты, в которых пострадало наибольшее количество людей, Мичиган занимает первое место, в основном из-за единственного инцидента в системе оказания медицинских услуг Trinity Health, в результате которого пострадали 3,3 человека.

По данным Ponemon Institute, устранение нарушений, затрагивающих медицинские организации, является наиболее дорогостоящим и требует самого длительного восстановления.

В среднем стоимость нарушенной записи в 2020 году составила 499 долларов, а восстановление заняло около 236 дней. Еще одним недостатком является тот факт, что медицинским учреждениям требуется 96 дней на выявление нарушения, больше, чем в любой другой отрасли.

Атаки программ-вымогателей

Хотя в отчете Bitglass инциденты взлома не разбиваются по их типам, на атаки программ-вымогателей, вероятно, приходится значительная часть.

Maze, Ryuk, REvil (Sodinokibi), SunCrypt, Snake и Clop - это лишь некоторые из групп вымогателей, которые атаковали больницы и медицинские учреждения.

В отчете Check Point ранее в этом году Ryuk и REvil были названы главными угрозами для сектора здравоохранения на глобальном уровне.

В конце октября 2020 года правительство США выпустило предупреждение об атаках программ-вымогателей Ryuk, нацеленных на больницы и поставщиков медицинских услуг. Ранее уведомление, в апреле, забило тревогу о вымогателях групп нарушающих больниц, используя уязвимость удаленного выполнения в импульсно Secure VPN серверов.

Новости о программах-вымогателях, поражающих различные больницы в США, просачивались в течение всего 2020 года, большинство из них - к концу года (1, 2, 3, 4, 5), а некоторые организации в конечном итоге платили хакерам сотни тысяч долларов США. вернуться к нормальной деятельности». ***(Ionut Ilascu. Rising healthcare breaches driven by hacking and unsecured servers // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/rising-healthcare-breaches-driven-by-hacking-and-unsecured-servers/). 17.02.2021).***

***

«Федеральное бюро расследований (ФБР) предупредило о тяжелых последствиях телефонных атак типа «отказ в обслуживании» (TDoS), а также предоставило меры, необходимые для смягчения их воздействия.

ФБР опубликовало это предупреждение в среду в качестве объявления государственной службы IC3 и уведомления частного сектора, выпущенного для организаций частного сектора в координации с DHS-CISA.

Нападения на службы экстренной помощи могут привести к гибели людей

TDoS-атаки - это ручные или автоматические злонамеренные попытки сделать телефонные системы недоступными путем блокировки входящих и исходящих вызовов, что может иметь ужасные последствия, если они будут направлены на службу 911 или аналогичные службы центра экстренного вызова.

«Цель состоит в том, чтобы как можно дольше удерживать отвлекающие звонки активными, чтобы перегрузить телефонную систему жертвы, что может задержать или заблокировать законные звонки в службу поддержки», - заявили в ФБР.

«Увеличение времени реагирования служб экстренной помощи может иметь ужасные последствия, включая гибель людей».

Злоумышленники могут координировать такие атаки по разным причинам, включая хактивизм, финансовую выгоду или преследование.

В то время как хактивисты могут злоупотреблять ими для пропаганды своих социальных или политических убеждений, злоумышленники могут и начали атаки TDoS для вымогательства у государственных и частных организаций.

Они также использовались в прошлом, чтобы помешать службам экстренной помощи отвечать на звонки на законные просьбы о помощи.

Агентства экстренной помощи также подвергались нападениям в прошлом

«IC3 стало известно об усилении тактики принуждения, применяемой субъектами, которая создала угрозу для служб экстренной помощи по всей стране», - говорится в сообщении ФБР от января 2013 года.

«В настоящее время угрозы переросли в атаки типа «отказ в обслуживании» телефонной связи (TDoS) против работодателей жертв, некоторые из которых были агентствами экстренных служб.

«В результате атак TDoS были заблокированы телефонные линии служб экстренной помощи, что не позволило им принимать и отвечать на законные вызовы службы экстренной помощи».

В отдельном конфиденциальном оповещении, разосланном в пункты приема звонков общественной безопасности (PSAP), центры экстренной связи и персонал в марте 2013 года, говорилось, что «[я] предполагается, что правительственные учреждения / службы экстренной помощи становятся «мишенью» из-за необходимости наличия функциональных телефонных линий.»

Как далее добавило ФБР во вчерашнем предупреждении, злоумышленники предоставляют услуги и инструменты TDoS злоумышленникам с различным уровнем опыта, что резко снижает уровень навыков, необходимых для запуска таких атак.

TDoS-атаки также сложно обнаружить, поскольку злоумышленники подделывают идентификатор вызывающего абонента при каждом звонке (в некоторых случаях предпочитая подделывать телефонные номера отделений полиции).

Это делает практически невозможным различение злонамеренных и законных вызовов…» ***(Sergiu Gatlan. FBI: Telephony denial-of-service attacks can lead to loss of lives // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/fbi-telephony-denial-of-service-attacks-can-lead-to-loss-of-lives/). 18.02.2021).***

***

«Количество предложений о доступе к сети и их медианные цены в публичных публикациях на хакерских форумах упали в последнем квартале прошлого года, но статистика не отражает реальный размер рынка начального доступа.

Данные компании Kela по разведке угроз показывают, что многие сделки фактически закрывались за закрытыми дверями, и эта тенденция сформировалась в последние месяцы.

Обманчиво маленькое предложение

По данным компании, более 240 предложений о продаже первоначального доступа к сети возникли в публичных обсуждениях на трех подпольных форумах. Четверть из них была произведена без ценника, что явно свидетельствовало о том, что транзакции совершаются в частных беседах.

Однако это число не включает предложение о доступе к более чем 500 сетям.gov и.edu (продано на аукционе за 25 биткойнов) и еще одно предложение для доступа к китайскому производителю электроники (просили 150 биткойнов). Ни один из них, похоже, не был закрыт из-за безумно высоких цен.

За 1500–2000 долларов покупатель мог получить администратора домена в компании среднего размера с несколькими сотнями сотрудников. Однако средняя цена в четвертом квартале составила 6 684 доллара, что больше, чем 4960 долларов, которые Kela увидела в сентябре 2020 года.

Совокупная сумма всех предложений, которые Kela наблюдала за отчетный период, составила 1 209 880 долларов США. Из них разносчики сообщили в открытых разговорах о заключении сделок на сумму всего 133 900 долларов, что составляет только 14% от всего предложения сети, которое увидела компания.

Частные дела

По сравнению с предыдущими данными, собранными в сентябре, это на 23% ниже. Однако это не дает точного представления о масштабах начального торгового доступа к сети. Как Kela упоминает, получая истинное чувство, насколько большой этот рынок «зависит только от брокеров и их будет указать продающиеся доступы или нет.»

Месяц за месяцем в четвертом квартале 2020 года было около 80 обращений к сети, в то время как в предыдущем периоде их было 108, что составляет 25% разрыв, который, вероятно, был вызван тем, что брокеры переводили переговоры с посредниками или покупателями в частные каналы, чтобы избежать взглядов посторонних. исследователи.

«Эта гипотеза основана на том факте, что многие брокеры первичного доступа обычно пишут, чтобы связаться с ними в частном порядке, чтобы получить информацию о других доступах, которые они готовы продать. Хотя такое поведение существовало всегда, в последние пару месяцев появилась более свежая тенденция - брокеры часто предлагают несколько вариантов доступа в одном потоке и просят потенциальных покупателей связаться с ними в частном порядке, чтобы получить весь список» - Kela

В качестве альтернативы, как и в случае с бизнесом вымогателей, некоторые продавцы начального доступа объявляют тип доступа, который им нужен для привлечения партнеров, и становятся филиалами, работающими за процент.

Подобные предложения не редкость. В другом брокер сообщил, что у них было «70 обращений к Citrix из стран первого уровня», чтобы предложить прибыльные цели.

Хотя и новые, и старые брокеры первичного доступа опубликовали свои предложения в четвертом квартале 2020 года, Kela говорит, что некоторые известные игроки перешли на частные сделки и лишь изредка объявляли о ценных и дорогих предложениях.

Один из этих участников, который был очень активен в течение лета, перечислил только два предложения в октябре и декабре: 35 000 долларов за доступ к государственному учреждению и 20 000 долларов за школьный округ в США.

Такое поведение характерно для брокеров, которые нашли постоянных покупателей, которые передали некоторые предложения. Поэтому они обратились к публичной части форума, чтобы закрыть сделку.

В основном доступ RDP, VPN, RCE

Что касается предоставляемого доступа, то в верхней части списка находятся эксплойты удаленного рабочего стола (RDP), VPN, удаленное выполнение кода и продукты Citrix. Это более 45% всех видов.

Среди менее распространенных типов доступа аналитик Kela по анализу угроз Виктория Кивилевич обнаружила программное обеспечение для мониторинга и устранения неисправностей DX NetOps и DX Spectrum, принадлежащее компании, которая управляла аэропортом.

Поскольку он может управлять всей ИТ-инфраструктурой, его можно использовать для бокового перемещения, чтобы поставить под угрозу всю сеть. Доступ через это ПО был продан за четыре дня.

Самые дорогие доступы (более 100 000 долларов), которые Kela увидела в четвертом квартале 2020 года, касались как государственных, так и частных организаций в США, Австралии, Мексике, Индии и Европе.

Среди пострадавших были ИТ-компании - скорее всего, поставщики управляемых услуг, обеспечивающие доступ к своим клиентам, телекоммуникационные компании, интернет-провайдеры, государственные учреждения и крупная нефтегазовая компания.

Некоторые из жертв были скомпрометированы через некоторое время после первоначального предложения доступа, как, например, в случае с Национальной комиссией по страхованию и гарантиям Мексики, объявленной на двух форумах на сумму не менее 70 000 долларов. В начале декабря программа-вымогатель LockBit зашифровала их компьютеры.

Торговцы доступом к сети продолжают разжигать кибератаки всех видов, в первую очередь программы-вымогатели. Среди наиболее активных из них:

Crasty - в основном предлагает доступ к Citrix / RDWeb организациям Австралии, Франции, США, а также компаниям из других стран, многие из которых являются университетами.

pshmm - продажа доступа к RMM в основном американским компаниям, использующим Zoho's ManageEngine Desktop Central

drumrlu / 3lv4n: обеспечивает множественный доступ, утверждая, что также скомпрометирует программное обеспечение VMware ESXi затронутых организаций.

Barf: обычно продает тип доступа RDP с правами пользователя компаниям из Франции, США, Бразилии, Испании, Италии и Германии.

7h0rf1nn: обычно предлагает RCE и веб-оболочки в сетях скомпрометированных компаний из образовательного, телекоммуникационного, финансового, страхового и спортивного секторов». ***(Ionut Ilascu. Hackers ask only $1,500 for access to breached company networks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-ask-only-1-500-for-access-to-breached-company-networks/). 11.02.2021).***

***

«Ведущая французская компания по кибербезопасности StormShield сообщила, что их системы были взломаны, что позволило злоумышленнику получить доступ к системе заявок в службу поддержки компании и украсть исходный код программного обеспечения межсетевого экрана Stormshield Network Security.

StormShield - французская компания, занимающаяся кибербезопасностью, которая разрабатывает брандмауэры UTM (Unified Threat Management), решения для защиты конечных точек и решения для безопасного управления файлами.

SNi40 от StormShield - единственный промышленный межсетевой экран, получивший сертификат безопасности первого уровня (CSPN) от Французского национального агентства безопасности информации (ANSSI).

StormShield раскрывает утечку данных

В новом сообщении по безопасности, выпущенном сегодня, StormShield сообщила, что их технический портал, используемый в качестве системы заявок в службу поддержки, был взломан и, возможно, позволял злоумышленникам просматривать технические обмены.

«Недавно группы Stormshield обнаружили инцидент безопасности, который привел к несанкционированному доступу к техническому порталу, который используется, в частности, нашими клиентами и партнерами для управления своими билетами в службу поддержки по нашим продуктам».

«Возможно, использовались личные данные и технические обмены, связанные с определенными учетными записями. Мы немедленно уведомили владельцев учетных записей на портале и уведомили французские власти. В качестве меры предосторожности мы сбросили пароли всех учетных записей, и мы применили дополнительные меры к порталу чтобы укрепить свою безопасность».

«Все заявки на поддержку и технические обмены в соответствующих учетных записях были рассмотрены, и результаты доведены до сведения клиентов», - сообщил StormShield в уведомлении по безопасности.

StormShield обнаружил, что злоумышленники получили доступ к некоторому исходному коду для своего исходного кода SNS (Stormshield Network Security) во

время атаки после дальнейшего расследования. Их исследования не указывают на то, что исходный код был изменен.

«Дальнейшее расследование этого инцидента выявило утечку некоторых частей исходного кода SNS (Stormshield Network Security). Эта информация также была передана нашим клиентам», - предупредил StormShield своих клиентов.

Поскольку прошивка Stormshield Network Security (SNS) поддерживает брандмауэры UTM компании, утечка исходного кода компании может облегчить злоумышленникам поиск ошибок, которые злоумышленники могут использовать для использования устройств. Эта утечка вызывает особую озабоченность, поскольку устройства StormShield SNS обычно используются правительством Франции, оборонными ведомствами и европейским рынком малого и среднего бизнеса.

В целях безопасности StormShield предполагает изменение сертификата подписи кода, используемого для обеспечения целостности выпусков и обновлений прошивки SNS (Stormshield Network Security).

Получив информацию об атаке, ANSSI выпустило рекомендацию по безопасности, в которой заявляет, что «решили поставить под наблюдение квалификации и одобрения продуктов SNS и SNI».

BleepingComputer обратился в StormShield с вопросами об атаке». ***(Lawrence Abrams. Hackers steal StormShield firewall source code in data breach // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hackers-steal-stormshield-firewall-source-code-in-data-breach/). 04.02.2021).***

***

«Как и любая другая компания в деловом мире, киберпреступники стремятся увеличить свои продажи. С помощью программ-вымогателей они нашли способ заставить жертв платить. И в своем стремлении кибератаки заимствуют методику у отделов продаж законных предприятий. Я заметил сходство между тактикой преступников с использованием программ-вымогателей и корпоративными продажами. Важно понимать сходство, потому что атаки программ-вымогателей не прекратятся в ближайшее время.

Киберпреступники годами переходят к законным бизнес-моделям. Киберпреступность как услуга позволяет неквалифицированным преступникам передавать свои бот-сети, фишинговые атаки и атаки программ-вымогателей более специализированным хакерам. Справочные службы, счета-фактуры и даже гарантии возврата денег стали нормой в криминальном подполье. Программы-вымогатели сами по себе стали настолько большим бизнесом, что кибербанды подвергают его лечению. Вот несколько способов, которыми злоумышленники копируют традиционные методы продаж:

Поиск и разведка

Первый шаг в привлечении клиентов - это определение вашей целевой аудитории. Для злоумышленников-вымогателей разведка похожа на традиционный поиск, когда они пытаются найти жертв, которых можно заставить подумать о платеже. Подобно законным предприятиям, киберпреступники стараются выяснить, какие организации и в каких секторах с наибольшей вероятностью в

конечном итоге заплатят выкуп, чтобы вернуть свои данные и услуги под свой контроль. Они будут использовать социальные сети, такие как LinkedIn и Twitter, чтобы найти сотрудников для таргетинга.

Запуск кампании

Киберпреступникам необходимо глубоко разбираться в организации, на которую они нацелены. Как и стандартные кампании по продажам, они обычно начинаются с прекрасного предлога. После того, как вредоносное ПО исчезнет, они проведут разведку в сети организации. Они ищут уязвимости, которые можно использовать, и где находятся критически важные активы и инфраструктура. Фишинговое электронное письмо должно быть тщательно обработано с использованием только правильного сообщения, побуждающего к действию - получатель должен открыть его и либо загрузить вложение, либо щелкнуть ссылку. Средняя открытая ставка для стандартных электронной почте маркетинговых кампаний 15% -25% с щелчком по ставке 2,5% по сравнению с 30% фишинговых писем, которые открыты.

Предоставьте образец

Чтобы заинтересованные клиенты превратились в реальных покупателей, маркетологи часто предоставляют образцы продукта или пробную версию. В атаках программ-вымогателей киберпреступники доказывают жертвам, что они взломали сеть, предоставив образец украденных данных. Часто киберпреступники предоставляют доказательства того, что ключи для разблокировки зашифрованных данных действительно работают. Киберпреступники обычно держат свое слово и возвращают данные, чтобы не подорвать свою репутацию. Одно исследование показало, что 58% жертв платят выкуп, а другое показало, что преступники не расшифровывают данные после получения платежа всего в 1% случаев.

Переговоры

Хотя многие продавцы нечасто снижают цены по просьбе покупателя, это происходит в ситуациях, когда рынок более подвижен, а воронка продаж ограничена. Киберпреступники-вымогатели рассчитывают договориться о цене, потому что знают, что данные не так ценны для кого-то еще. Если организация не платит, киберпреступник может опубликовать данные, что смущает жертву. Но преступники предпочли бы снизить цену, чем вообще не получить деньги - большая потеря, когда средняя цена вымогателя превышает 110 000 долларов.

Вот несколько рекомендаций, которые помогут организациям избежать попадания программ-вымогателей и минимизировать ущерб, если они есть:

Задраить люки

Организации должны стараться не допускать проникновения вредоносных программ в свои сети. По данным Verizon, каждое пятое нарушение связано с фишингом, поэтому обучение сотрудников распознаванию фишинговых писем и использованию средств защиты от фишинга и вредоносных программ имеет решающее значение. Кроме того, следите за обновлениями и исправлениями приложений и операционной системы, чтобы предотвратить проникновение злоумышленников через уязвимое программное обеспечение - 60% нарушений связаны с программным обеспечением без исправлений.

Назад к основам

Не забывайте делать частые и регулярные резервные копии данных и хранить их отдельно от обычных сетей, которые могут подвергнуться атакам программ-вымогателей. Резервные копии должны находиться в месте, недоступном для злоумышленников, например, в воздушном зазоре или физически отделенном от сети, подключенной к Интернету. Это требует обновлений вручную, но это самый безопасный подход.

Настольные упражнения

Организации должны практиковать планирование непрерывности бизнеса, чтобы быть готовыми к атаке программ-вымогателей и быстро восстановиться. Это означает, что все, от технических специалистов и специалистов по безопасности до юристов, финансов и PR, на одной странице. Команды должны проработать разные сценарии и отработать шаги, которые им необходимо будет предпринять в случае атаки. Эти настольные упражнения следует выполнять не реже одного раза в квартал. Команды также должны попрактиковаться в восстановлении данных из резервной копии и убедиться, что они действительно получают данные, когда им нужно, и что они знают, где хранятся ключевые данные.

Для киберпреступников общий адресный рынок программ-вымогателей трудно измерить, но он действительно велик - потенциальной целью может быть любая компания. Программы-вымогатели прямо сейчас могут поразить такие важные отрасли, как правительство, здравоохранение и образование, но у каждой организации есть свой порог в отношении бизнес-операций и данных, которые они готовы платить, чтобы не потерять». ***(Marcus J. Carey. How cybercriminals use sales best practices in ransomware attacks // BNP Media (https://www.securitymagazine.com/blogs/14-security-blog/post/94392-how-cybercriminals-use-sales-best-practices-in-ransomware-attacks). 21.02.2021).***

***

«Удаленная работа продолжает способствовать росту фишинга и кибератак, особенно в США.

Когда дело доходит до уплаты выкупа при атаке программы-вымогателя, требования растут. Тем не менее, согласно опросу, опубликованному в понедельник, многие компании, заплатившие выкуп, не получили ключ дешифрования.

На самом деле, согласно отчету, фишинговые атаки на тему пандемии, постоянное нападение программ-вымогателей и рост числа удаленных сотрудников по всему миру - все это вместе сделало последние 12 месяцев особенно жестокими для специалистов по информационной безопасности.

В отчете Proofpoint State of the Phish за 2021 год опрошено 600 профессионалов в области информационной безопасности в семи странах: Австралии, Франции, Германии, Японии, Испании, Великобритании и США; включены основные моменты дополнительного опроса 3 500 взрослых работников из тех же стран, проведенного третьей стороной; и проанализировали более 60 миллионов смоделированных фишинговых атак, чтобы прийти к заключению, сообщила компания.

Дополнительный всплеск требований о выкупе

По словам Proofpoint, из 75 процентов компаний, которые ответили на отчет State of the Phish, заявив, что они были заражены программой- вымогателем, более половины решили заплатить выкуп, чтобы вернуть свои данные. Из той половины, кто заплатил, только 60% получили доступ к своим данным. Остальные 40 процентов получили дополнительный выкуп, что на 320 процентов больше, чем в прошлом году.

Вместо того чтобы реагировать после того, как они потеряли контроль над своими данными, Гретель Иган, старший специалист по вопросам безопасности и стратег по обучению в Proofpoint, сказала Threatpost, что организациям необходимо принимать решения о том, как реагировать задолго до взлома.

«Реакция на заражение программой-вымогателем - очень индивидуальный вопрос, - сказал Иган. «Масштаб заражения, влияние на операции и размер выкупа, вероятно, повлияют на окончательное решение о том, как бороться с атакой. Но передовой практикой является наличие тщательно подготовленного и протестированного ответа до того, как начнется атака программы-вымогателя, которая учитывает ряд различных сценариев использования программ-вымогателей. Очень важно оценить риск по сравнению с вознаграждением за совершение платежа и альтернативы, которые они могут использовать.

Количество попыток фишинга компаний

Отчет показывает резкий рост попыток фишинга, особенно в США, где количество атак увеличилось на 14 процентов по сравнению с прошлым годом и на 30 процентов больше, чем в остальном мире.

И пока развертываются массовые фишинговые атаки по широкой сети, злоумышленники становятся еще лучше в борьбе с более целенаправленными махинациями социальной инженерии, такими как целевой фишинг, китобойный промысел и атаки компрометации деловой электронной почты (BEC).

Электронная почта по-прежнему является предпочтительным каналом для фишеров, потому что недостаточно обученные сотрудники упрощают эту задачу, поясняется в отчете, но специалистам по безопасности также необходимо учитывать другие схемы социальной инженерии, с которыми сталкиваются организации, такие как использование социальных сетей, голосовая почта «вишинг», SMS / text фишинг или «smishing», и даже вредоносные USB-файлы.

«Организаторы угроз по всему миру продолжают нацеливаться на людей с помощью гибких, актуальных и сложных коммуникаций, в первую очередь через канал электронной почты, который остается основным вектором угроз», - сказал Алан ЛеФорт, старший вице-президент и генеральный менеджер отдела обучения безопасности для Proofpoint. «Обеспечение понимания пользователями того, как выявлять попытки кибератак и сообщать о них, несомненно, критически важно для бизнеса, особенно когда пользователи продолжают работать удаленно - часто в менее защищенной среде. Хотя многие организации заявляют, что проводят обучение своих сотрудников по вопросам безопасности, наши данные показывают, что большинство из них делает недостаточно».

Тренинги по вопросам безопасности

В то время как 90 процентов респондентов в США указали, что их сотрудники перешли на удаленную работу в 2020 году, только 29 процентов из них

предложили сотрудникам какое-либо обучение безопасным привычкам удаленной работы, сказал Proofpoint, создав совершенно новое место для охоты на фишинговых злоумышленников практически в мгновение ока.

В отчете говорится, что за 12-месячный период Proofpoint было зарегистрировано более 800 000 активных фишинговых атак с использованием учетных данных и 35 000 фишинговых писем, содержащих вредоносные программы, включая троянов удаленного доступа (RAT), клавиатурных шпионов и постоянные угрозы повышенной сложности (APT).

«Результаты, касающиеся удаленной работы в США, открывают глаза», - добавил ЛеФорт. «Почти все опрошенные нами американские специалисты в области информационной безопасности заявили, что в прошлом году они поддержали новую модель удаленной работы как минимум для половины сотрудников своей организации. И все же менее трети этих респондентов заявили, что рабочих обучили методам безопасности, связанным с работой из дома».

В то же время три четверти американских рабочих заявили, что они позволяют своим друзьям и родственникам получать доступ к служебным устройствам, чтобы делать такие вещи, как делать покупки в Интернете и играть в игры.

«Эти пробелы представляют собой значительный риск и усиливают потребность в инициативах по обучению вопросам безопасности, ориентированных на удаленную рабочую силу», - сказал ЛеФорт.

В отчете подчеркивается, что тренинг по вопросам безопасности работает. Proofpoint обнаружил, что 80 процентов организаций, участвовавших в опросе, обнаружили, что обучение «снижает уязвимость к фишингу». При тестировании, как выяснил Proofpoint, больше всего заботились о безопасности группы закупок, тогда как сотрудники технического обслуживания и оборудования получили худшие оценки.

Как предотвратить программы-вымогатели и фишинг

Иган также предложил превентивные меры безопасности, такие как специальный расширенный шлюз безопасности электронной почты, надежное резервное копирование данных и последовательное внесение исправлений для обновления систем.

«Кроме того, для успеха большинства атак требуется человеческое взаимодействие - и они в основном нацелены на конкретных людей», - пояснил Иган. «Мы рекомендуем проводить непрерывное обучение по вопросам безопасности для каждого сотрудника и подрядчика, имеющего доступ к корпоративным системам. Некоторые варианты программ-вымогателей будут запрашивать оплату у человека, поэтому важно, чтобы сотрудники знали, что нельзя делать никаких платежей самостоятельно, и сообщать о них своим руководителям».

Есть хорошие новости. Общее количество зарегистрированных случаев заражения программами-вымогателями осталось примерно на том же уровне, и Proofpoint сообщила, что количество заражений вредоносным ПО в результате фишинга снизилось на 17 процентов. Более того, количество респондентов, сообщающих о прямых финансовых потерях, снизилось на 47%, что, как добавлено

в отчете, «может указывать на то, что организации внедрили более строгие превентивные меры против этих типов атак», и, что еще лучше, эти меры работают». ***(Becky Bracken. Ransomware Demands Spike 320%, Payments Rise // Threatpost (https://threatpost.com/ransomware-demands-spike-payments-rise/163744/). 08.02.2021).***

***

«Поставщик антивирусных решений, компания Emsisoft сообщает, что неизвестная третья сторона получила доступ к базе данных, содержащей технические логи.

Проблема заключалась в том, что тестовая система оказалась неверно сконфигурирована и доступна через интернет, а вместе с ней упомянутая БД. Эта система использовалась для оценки и сравнительного анализа хранения и управления данными логов, которые генерируют продукты и сервисы Emsisoft. Из-за ошибки сотрудников, БД стала доступна для всех желающих 18 января 2021 года, а утечку обнаружили и устранили только 3 февраля 2021 года.

Сообщается, что конфиденциальной информации в базе было немного: 14 адресов электронной почты, принадлежащие семи различным организациям. Однако БД хранила множество продакшен-логов, а расследование показало, что по меньшей мере один человек «получил доступ к некоторым или всем данным, содержащимся в этой базе данных».

«Украденные данные состоят из технических логов, создаваемых нашим защитным ПО в ходе обычной работы, например, протоколов обновления. Обычно [такие логи] не содержат никакой личной информации, включая пароли, хэши паролей, имена учетных записей пользователей, информацию для выставления счетов, адреса и так далее», — уверяют в компании.

Вышеупомянутые 14 адресов электронной почты, которые хранились в базе данных, попали туда через логи сканеров, так как в почтовых клиентах пользователей были обнаружены вредоносные электронные письма». ***(Мария Нефёдова. Компания Emsisoft сообщила об утечке данных // Хакер (https://xakep.ru/2021/02/11/emsisoft-leak/). 11.02.2021).***

***

«Специалисты Group-IB обнаружили 706 мошеннических сайтов, стилизованных под официальный ресурс Rakuten Viber, где мошенники обещали пользователям розыгрыши и призы (на самом деле стремясь похитить их деньги).

Так как Group-IB заключила с Rakuten Viber партнерское соглашение для защиты бренда, компания ведет мониторинг подозрительной активности с использованием бренда Viber, отслеживая такие источники, как доменные имена, контекстную рекламу, поисковую выдачу, магазины мобильных приложений, соцсети, базы с утечками данных и даркнет. Кроме того, на вредоносные ресурсы жалуются сами пользователи, отмечая аккаунты, рассылающие спам или ссылки на мошеннические сайты.

В итоге было подсчитано, что в 2020 году количество мошеннических ресурсов, имитирующих сайт Viber, выросло на 190% по сравнению с предыдущим годом. Всего же на территории РФ в прошлом году было обнаружено более 706 мошеннических сайтов, чью деятельность практически полностью удалось прекратить — было закрыто 98% из этих ресурсов.

Первая волна мошенничества началась в феврале и была связана с пандемией, остальные выявленные случаи в большей степени касались годовщины компании Rakuten Viber — в 2020 году мессенджер отпраздновал свое десятилетие. Мошенники создавали сайты с ложной информацией о розыгрышах в мессенджере и делились ссылками на них в групповых и личных чатах Viber, а также за его пределами.

Для привлечения пользователей к своим сайтам злоумышленники обычно используют целевую рассылку сообщений с «приманкой» в виде конкурса, розыгрыша призов или лотереи. Причем, в зависимости от места нахождения потенциальной жертвы (мошенники считывают IP, доменную зону и другие данные) «приманка» рассылается на языке жертвы и идет от имени популярного в стране бренда или персоны.

Согласно оценкам Group-IB, на атаки и мошенничество с незаконным использованием брендов в мире пришлось 54% от всех киберпреступлений, которые были совершены в период за первые 9 месяцев 2020 года. В них выделяется две группы: фишинговые ресурсы, которые собирают учетные данные или платежную информацию жертв (16%) и интернет-мошенничество, мотивирующее пользователей добровольно переводить деньги злоумышленникам под видом оплаты интернет-заказов, получения компенсаций, розыгрышей призов или фейковых акций от известных брендов (38%)». ***(Мария Нефёдова. Более 700 мошеннических ресурсов имитировали сайт Viber // Xakep (https://xakep.ru/2021/02/08/viber-scam/). 08.02.2021).***

***

«Специалистам ИБ-компании Cisco Talos удалось пообщаться с оператором вымогательского ПО LockBit, который проводил все вредоносные операции в одиночку. Хакер рассказал о своем modus operandi (жертвах, инструментах и пр.) и о том, что толкнуло его на путь киберпреступности. Кроме того, он поведал о нелегкой судьбе исследователя безопасности в его родной стране, которой, по мнению Cisco Talos, является Россия.

В ходе интервью оператор LockBit, назвавшийся Алексом (по мнению Cisco Talos, он живет в Сибири и ему немного за тридцать), сообщил, что является исследователем-самоучкой, специализирующимся на тестировании на проникновение, сетевой безопасности и разведке.

Будучи еще студентом, Алекс получил работу в IT-компании, но быстро разочаровался, так как почувствовал, что «российская кибериндустрия не оценила должным образом» его способности.

«Его разочарование стало очевидным, когда во время наших разговоров он пренебрежительно отозвался о нескольких известных российских компаниях, занимающихся кибербезопасностью. Он также заметил, что “на Западе я, вероятно,

мог бы работать по белому и легко зарабатывать…" предполагая, что именно недооценка его способностей и низкая заработная плата заставили его участвовать в неэтичной и преступной деятельности», – сообщается в отчете Cisco Talos.

Алекс даже привел несколько примеров такой «недооценки» – отказ принимать его отчеты о проблемах с безопасностью на нескольких сайтах, в том числе в российской социальной сети. Его «благие намерения были проигнорированы», заявил Алекс, что и толкнуло его на путь киберпреступности.

Заниматься поиском уязвимостей и участвовать в программах bug bounty Алекс также считает гиблым делом, так как компании делают все возможное для того, чтобы не платить исследователям. Но специалисты Cisco Talos уверены, что молодой человек ошибается, поскольку его заявление совсем не соответствует результатам их наблюдений. Вероятнее всего, он просто наслушался неправдивых рассказов других киберпреступников.

Примечательно, что решение Алекса стать оператором вымогательского ПО было вызвано не только желанием финансовой выгоды. Хотя кибервымогательство действительно приносит большую прибыль, молодой человек также хотел показать компаниям, чем чревато недостаточное обеспечение безопасности данных.

Как отметил Алекс, «для киберпреступников лучшей страной является Россия», а лучшими жертвами – компании в США и Европе, которые платят «быстрее и больше», чем компании в постсоветском пространстве. Дело в том, что в случае с западными компаниями выплаты вымогателям покрывает страховка. Кроме того, жертвы в Европе боятся утечки своих данных из-за штрафов, которыми это грозит в рамках «Общего регламента по защите данных» (GDPR).

Киберпреступники часто склонны оправдывать свои действия постфактум, даже если в преступлении не было реальной моральной двусмысленности. «В данном случае на путь киберпреступности его (Алекса – ред.) толкнуло отсутствие работы, которая соответствовала бы его запросам. Недооценка способностей, негодование и отсутствие экономического стимула часто являются причинами, толкающими на путь киберпреступности, и это история является ярким примером», – подытожили эксперты». ***(Оператор LockBit: Лучшей страной для киберпреступника является Россия // SecurityLab.ru (https://www.securitylab.ru/news/516256.php). 05.02.2021).***

***

«Государственный секретарь по цифровому переходу Седрик О заявил в среду, что французские больницы подверглись 27 крупным кибератакам в 2020 году, напомнив, однако, что все французское общество и экономика живут под этой угрозой. Во Франции «в 2020 году было 27 крупных нападений на больницы, с 2021 года происходило одно нападение в неделю», - ответил Седрик О, опрошенный в Сенате во время вопросов правительству об атаке, направленной на больничный центр. Из Дакса (Ланды) в ночь с 8 на 9 февраля. "С 9 февраля агенты Ансси (Национальное агентство безопасности информационных систем) прибыли в больницу Дакс на месте. Два дня назад они отправились в Вильфранш-сюр-Сон (Рона, жертва вымогателя RIUK в понедельник утром), где я буду через несколько дней», - добавил он.

По словам госсекретаря, 110 французских больниц прошли «аудиты безопасности» благодаря поддержке Ансси, а «11 из них сопровождаются на повседневной основе». Столкнувшись с быстрым развитием угрозы, которая также затрагивает предприятия, государственные учреждения и сообщества в нескольких странах, исполнительная власть готовится объявить о новых мерах в четверг. «Что касается юридического ответа, я хотел бы выделить два недавних успеха, - продолжил Седрик О, имея в виду демонтаж вредоносного ПО Emotet в конце января и арест на прошлой неделе хакеров, подозреваемых в связях с программой-вымогателем Egregor.благодаря сотрудничеству между французскими службами, французскими и американскими судами и нашими европейскими партнерами».

Emotet, в частности, использовался во Франции для нападения на определенные службы Министерства юстиции, магистратов и юристов в Париже в сентябре прошлого года и считается одним из крупнейших векторов заражения программ-вымогателей. Egregor, со своей стороны, использовался в атаке на ежедневную газету Ouest France в конце ноября, сказал Седрик О. «Атаки на больницы показывают, что атака вымогателя может иметь последствия для жизни людей. Пациенты в реальной жизни мире, подвергая опасности жизни пациентов», - заявил Ансси в начале февраля в своем отчете». ***(Cybersécurité des hôpitaux: «27 attaques majeures en 2020 et une par semaine en 2021» // Le Figaro (https://www.lefigaro.fr/flash-eco/cybersecurite-des-hopitaux-27-attaques-majeures-en-2020-et-une-par-semaine-en-2021-20210217). 17.02.2021).***

***

«Список французских больниц, местных властей и компаний, пострадавших от кибератак, сейчас растет с каждым днем. В 2020 году киберпреступность увеличилась в четыре раза по сравнению с предыдущим годом, если мы посмотрим на количество вмешательств со стороны Национального агентства по безопасности информационных систем (Anssi), отвечающего за государственную киберзащиту.

Кризис со здоровьем, конечно, ничему не помог, но он не является причиной этого ускорения. Все страны и отрасли сталкиваются с этим по той простой причине, что преступники в течение многих лет находили в киберпространстве относительно недорогие, но, с другой стороны, очень прибыльные средства осуществления незаконной деятельности. Применяя сейчас промышленно развитые методы атак, часто изощренные, иногда подкрепленные геополитическими соображениями, они наносят удары любой ценой, используя в своих интересах хрупкость предприятий, медицинских учреждений, сообществ, ассоциаций или простых людей. С серьезными эксплуатационными и экономическими последствиями для всех пострадавших.

Поэтому, чтобы ответить на экспоненциальный рост этих серьезных угроз, французское государство решило ускорить свою стратегию киберзащиты. Представленный в четверг президентом Эммануэлем Макроном, он направлен на повышение общего уровня защиты государственных и частных субъектов, а также на стимулирование развития сектора кибербезопасности во Франции.

Усиление обнаружения

В рамках плана восстановления и инвестиционной программы на будущее Франция инвестирует к 2025 году дополнительный миллиард евро в эту национальную стратегию. Они будут добавлены к финансированию, уже предоставленному для помощи в цифровом переходе администраций. Дополнительные ресурсы (136 миллионов евро) будут выделены компании Anssi, в частности, для проведения диагностики безопасности с медицинскими учреждениями и местными властями, полагаясь на доверенных местных игроков. Решения будут протестированы на пилотных объектах (территория, больница), а затем тиражированы в национальном масштабе. Ансси также хочет усилить средства обнаружения атак, создав региональные CERT (Computer Emergency Response Team),

Для развития своих защитных возможностей Франция также рассчитывает на разработку передовых технологических решений. На это будет направлено пятьсот миллионов евро за счет финансирования проектов исследовательских центров (Inria, CNRS, CEA и др.) Или совместных проектов с частными компаниями. Только передовые технологии смогут, например, помочь малым и средним предприятиям автоматизировать безопасность своих информационных систем, эффективно защищать подключенные объекты или решать специфические проблемы определенных секторов.

Для государства это также важный вопрос экономического развития и суверенитета. К 2025 году он хочет в четыре раза увеличить оборот сектора (до 25 миллиардов евро) и удвоить количество созданных рабочих мест. Сектор кибербезопасности страдает от нехватки профилей и определенной непривлекательности, особенно среди девочек. Чтобы исправить это, в стратегии особое внимание уделяется тренировкам. Как только будут определены приоритетные потребности, будут созданы и профинансированы новые учебные курсы и новые магистры». ***(Ingrid Vergara. Face à la multiplication des attaques, la France accélère sa stratégie de cybersécurité // Le Figaro (https://www.lefigaro.fr/secteur/high-tech/face-a-la-multiplication-des-attaques-la-france-accelere-sa-strategie-de-cybersecurite-20210217). 17.02.2021).***

***

«Подразделение IBM Security представило ежегодный индекс угроз информационной безопасности «X-Force Threat Intelligence Index 2021», который показывает, как менялся характер кибератак в 2020 г. – в период пандемии Covid-19, когда злоумышленники пытались извлечь выгоду из беспрецедентной социально-экономической ситуации и вызовов политического и делового характера.

Согласно наблюдениям IBM Security X-Force, в минувшем году злоумышленники чаще атаковали те организации, которые играют наиболее важную роль в глобальной борьбе с Covid-19. Так количество кибератак в сфере здравоохранения, производства и энергетики удвоилось по сравнению с предыдущим годом. Причем основной целью стали компании, для которых даже небольшая остановка деятельности может оказаться критичной, потому что сведет на нет усилия врачей или прервет жизненно важные поставки. Производство и

энергетика вышли в число отраслевых лидеров среди мишеней в 2020 г., уступив по количеству кибератак только финансовому сектору и сфере страхования (PDF, RU). Отчасти этому способствовал практически 50% рост числа уязвимостей в промышленных системах управления (Industrial Control Systems, ICS), которые активно используются и в производстве, и в энергетике.

Отчет X-Force Threat Intelligence Index составляется по результатам ежедневного мониторинга более 150 млрд событий из сферы ИБ более чем в 130 странах мира. В дополнение к этому данные поступают из разных источников внутри IBM, включая IBM Security X-Force and Incident Response, X-Force Red, IBM Managed Security Services, а также предоставляются компаниями Quad9 и Intezer, которые участвовали в составлении отчета за 2021 г.

Ключевые выводы отчета:

Киберпреступники выстраивают тактики на базе общепринятых принципов использования гибридных облаков. Согласно данным Intezer, количество вредоносного ПО на базе Linux в прошлом году увеличилось на 40%, а количество вредоносного ПО на базе Go выросло в шесть раз за первое полугодие 2020 г. Это говорит о том, что злоумышленники ускоренными темпами осваивают атаки, используя Linux. Следуя принципу для гибридных облачных сред «пиши код один раз, запускай где угодно», злоумышленники создают вредоносное ПО, которое легко запускать на разных платформах, в том числе и в облачной инфраструктуре.

Пандемия выделила самые подделываемые бренды. В 2020 г. люди были вынуждены соблюдать дистанцию и работать из дома, а в десятку самых подделываемых брендов вошли разработчики средств для совместной работы, такие как Google, Dropbox и Microsoft, а также онлайн-магазины и сопутствующие компании, такие как Amazon и PayPal. YouTube и Facebook – основные источники новостей в прошлом году – тоже оказались в начале списка. Впервые в истории компании в рейтинге самых подделываемых брендов в 2020 г. на седьмом месте оказался бренд Adidas. Скорее всего, причиной тому был высокий спрос на две линейки кроссовок.

Владельцы вирусов-шифровальщиков ищут более выгодные бизнес-модели. Такие вредоносы были задействованы практически в каждой четвертой атаке, выявленной специалистами X-Force в 2020 г. Причем всё чаще в них применяется тактика двойного вымогательства. По оценке X-Force, самой активной группой вирусов-шифровальщиков в прошлом году стала Sodinokibi, использовавшая эту тактику. С ее помощью злоумышленники собрали свыше 123 млн. долл., причем почти две трети жертв соглашались заплатить выкуп.

В условиях пандемии Covid-19 многие компании стремились ускорить переход в облако. Согласно недавнему исследованию Gartner, почти 70% организаций, уже использующих облачные сервисы, планируют увеличить расходы на облачные технологии после сбоев в работе, вызванных Covid-19. Надо отметить, что 90% всех облачных вычислений сейчас осуществляется на базе Linux, а отчет X-Force показал, что за последнее десятилетие количество вредоносного ПО для Linux выросло в шесть раз. Это значит, что облачные среды могут стать основной целью злоумышленников.

По оценкам IBM, с развитием вредоносного ПО с открытым кодом злоумышленники могут искать дополнительные возможности увеличения маржи за счет возможного сокращения расходов, повышения эффективности и масштабирования наиболее успешных вариантов атак. Отчет показал, что различные атакующие группы, такие как APT28, APT29 и Carbanak, переключаются на ПО с открытым кодом, а значит количество атак на облачные среды в ближайшем году возрастет.

Результаты отчета также показали, что злоумышленники используют расширяемые вычислительные мощности облачных сред, сильно увеличивая плату за облачное потребление у своих жертв. В 2020 г. специалисты Intezer обнаружили более 13% нового кода в категории вредоносного ПО на базе Linux для криптомайнеров.

Поскольку злоумышленники обратили пристальное внимание на облачные технологии, X-Force рекомендует организациям всерьез рассмотреть возможность применения стратегии нулевого доверия в целях защиты данных.

Отчет показал, что киберпреступники предпочитают выдавать себя за бренды, которым доверяют потребители. Adidas считается одним из самых влиятельных брендов в мире, и этим воспользовались злоумышленники. Киберпреступники пытались заманить покупателей, мечтающих о кроссовках бренда, на поддельные сайты. Как только жертва попадала на сайт-подделку, ее убеждали совершить покупку и предоставить банковские или учетные данные – либо при посещении сайта на устройство жертвы устанавливалось вредоносное ПО.

В отчете говорится о том, что большая часть случаев обмана с брендом Adidas связана с кроссовками серий Yeezy и Superstar. Как сообщалось ранее, объем продаж модели Yeezy достиг 1,3 млрд. долл. в 2019 г. Это одна из самых продаваемых линеек у компании Adidas. Скорее всего, злоумышленники учли ажиотаж, связанный с выпуском новой серии кроссовок в начале 2020 г., и решили получить с него свою долю выручки.

Согласно отчету, в 2020 г. стало больше атак с использованием вирусов-шифровальщиков, чем было в 2019 г. Причем почти 60% всех вымогательских атак, выявленных специалистами X-Force, применялись по принципу двойного вымогательства, когда злоумышленник не просто шифрует данные, но еще и угрожает опубликовать их в сети, если выкуп не будет выплачен. В 2020 г. 36% случаев утечки данных, обнаруженных X-Force, были связаны с использованием вирусов-шифровальщиков, и сюда же относятся случаи предполагаемой кражи данных. То есть атаки, связанные с кражей данных, и вымогательские атаки начинают сливаться в одну категорию.

Для противостояния подобным агрессивным нападениям X-Force рекомендует компаниям ограничивать доступ к конфиденциальной информации и защищать привилегированные учетные записи с большими полномочиями, используя системы управления правами доступа (PAM) и управления учетными записями пользователей (IAM).

Другие важные выводы X-Force Threat Intelligence Index:

Уязвимости чаще становятся причиной взлома, чем фишинг. Отчет показал, что чаще всего злоумышленникам удавалось проникнуть в системы жертвы, используя уязвимости (35%), и этот метод впервые за многие годы стал более эффективным, чем фишинг (31%).

Европа сильнее пострадала от кибератак в 2020 г. На ее долю пришелся 31% всех атак, выявленных специалистами X-Force – это больше, чем в любом другом регионе. А число атак вирусов-шифровальщиков в Европе резко выросло. Кроме того, в Европе было больше атак со стороны инсайдеров, чем в других регионах – в два раза больше, чем в Северной Америке и в Азии вместе взятых». ***(Уязвимости впервые за много лет обошли фишинг в рейтинге методов взлома // Компьютерное Обозрение (https://ko.com.ua/uyazvimosti_vpervye_za_mnogo_let_oboshli_fishing_v_rejtinge_metodov_vzloma_136442). 24.02.2021).***

***

«В настоящее время проводится почтовая фишинговая кампания AOL с целью кражи логина и пароля пользователей путем предупреждения получателей о том, что их учетная запись будет закрыта.

В то время как большинство людей используют Gmail, Outlook или другие современные бесплатные почтовые службы, многие пожилые люди продолжают использовать AOL просто потому, что они привыкли к этой службе и считают ее слишком сложной для перехода на новую почтовую службу.

К сожалению, это также делает их основными целями для фишинговых атак, которые, по моему опыту, имеют тенденцию легче проскальзывать через фильтры электронной почты AOL, чем фильтры других сервисов, таких как Gmail.

На этой неделе со мной связались двое старших членов семьи, получившие письмо со страшной темой, в котором говорилось, что их «Почтовый ящик закроется через 3 дня, войдите в систему для повторной активации».

Боясь, что учетные записи электронной почты, которые они использовали почти 25 лет, будут закрыты, они переслали мне письмо и попросили совета.

В электронном письме говорилось, что им необходимо войти в систему и подтвердить свою учетную запись в течение 72 часов, иначе AOL деактивирует их учетную запись.

"Мы не хотим прощаться!"

«Мы заметили, что вы в последнее время не обновляли информацию о своей учетной записи, и, поскольку ваша безопасность является нашим главным приоритетом, мы планируем закрыть эту учетную запись как можно скорее. Если вы не предпримете никаких действий в ближайшее время, это займет 3 дня. Если вы не подтвердите эту учетную запись, он будет закрыт через 72 часа», - предупреждает фишинговое письмо AOL.

В письме была ссылка на плохо сконструированную фишинговую целевую страницу AOL, предлагающую посетителям войти в AOL.

После отправки учетных данных AOL в форму украденные учетные данные отправляются злоумышленникам, а пользователь перенаправляется на стандартную страницу входа в AOL.

Поскольку я старался рассказать членам семьи о фишинг-мошенничестве и о том, на что следует обращать внимание, члены моей семьи не попали на эту аферу.

К сожалению, многие люди, возможно, не получили такого же образования и, скорее всего, введут свои данные для входа в AOL…». ***(Lawrence Abrams. Beware: AOL phishing email states your account will be closed // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/beware-aol-phishing-email-states-your-account-will-be-closed/). 28.02.2021).***

***

«Исследователи безопасности, анализирующие несколько наборов вредоносных электронных писем, считают, что они обнаружили активность, принадлежащую ранее не идентифицированному субъекту, который соответствует описанию повышенной постоянной угрозы (APT).

Актер получил имя LazyScripter и ведет активную деятельность с 2018 года, используя фишинг для нацеливания на лиц, ищущих иммиграцию в Канаду для работы, авиакомпаний и Международной ассоциации воздушного транспорта (IATA).

Инфраструктура, поддерживающая эту долгосрочную кампанию, все еще активна, и субъект продолжает развиваться, обновляя свои наборы инструментов.

Использование проектов с открытым исходным кодом

Последняя деятельность LazyScripter включает использование свободно распространяемых вредоносных программ Octopus и Koadic. Оба были доставлены через вредоносные документы и ZIP-архивы, содержащие встроенные объекты (VBScript или пакетные файлы), а не макрокод, часто встречающийся при фишинговых атаках.

Исследователи из Malwarebytes также обнаружили другие примеры, когда злоумышленник сбрасывал другие трояны удаленного доступа (RAT), общие для нескольких хакерских групп: LuminosityLink, RMS, Quasar, njRat и Remcos.

По словам исследователей, LazyScripter перешел на тактику двойного RAT после первоначального использования постэксплуатационной структуры PowerShell Empire. Исследователи назвали погрузчики для этих грузов KOCTOPUS и Empoder соответственно.

Как правило, вредоносные документы содержат один или два встроенных объекта со значками, представляющими собой файлы PDF, Microsoft Word / Excel; на самом деле это пакетные, исполняемые или VBScript-варианты загрузчиков KOCTOPUS и Empoder.

KOCTOPUS, используемый для развертывания Octopus и Koadic и обеспечения их постоянства в системе, сильно запутывается с помощью инструмента BatchEncryption.

Общий процесс компрометации через KOCTOPUS включает в себя обход функции безопасности контроля учетных записей (UAC) в Windows, отключение продуктов безопасности Microsoft и загрузку RMS или LuminosityLink RAT.

Наборы инструментов для хостинга на GitHub

Интересно, что LazyScripter разместил свои наборы инструментов на GitHub - тактика, использовавшаяся в прошлом группой APT, связанной с Ираном.

Malwarebytes обнаружил три аккаунта, связанных с LazyScripter. Два из них - LIZySARA и Axella49 - были удалены в январе, но третий (OB2021) появился в начале месяца, 2 февраля, и продолжает действовать.

Некоторые из электронных приманок, по-видимому, специально разработаны для авиакомпаний, которые используют программное обеспечение BSPLink, решение IATA для своего плана биллинга и расчетов (BSP), которое позволяет компаниям:

Управляйте сбором и платежами по всему миру в едином процессе

Автоматическое восстановление данных сверки доходов за счет передачи одного файла

Автоматизируйте управление ADM / ACM или возвратами

Управляйте стимулами продаж с помощью дополнительной услуги Global Net Remit 5 с помощью того же процесса расчетов

Разнообразие приманок

Приманка изменилась недавно, «чтобы имитировать новую функцию, недавно представленную IATA, которая называется IATA ONE ID (инструмент бесконтактной обработки информации о пассажирах)», - говорится в сегодняшнем подробном техническом отчете Malwarebytes.

Компания добавляет, что это показатель того, что злоумышленник адаптирует свой набор инструментов для работы с новыми системами, разработанными IATA. Более обширная коллекция приманок LazyScripter включает следующее:

• Безопасность IATA (безопасность Международной ассоциации воздушного транспорта)

• BSPlink Updater или Upgrade (BSPlink - это глобальный интерфейс для туристических агентств и авиакомпаний для доступа к IATA BSP)

• IATA ONE ID

• Комплекты поддержки пользователей для пользователей IATA

• Туризм (ЮНВТО)

• COVID-19

• Обновления Microsoft

• Информация о вакансии

• Канадская программа повышения квалификации

• Виза в Канаду (CanadaVisa.com - это онлайн-представительство иммиграционной юридической фирмы Campbell Cohen)…

Для управления и контроля (C2) LazyScripter использует пять поддоменов на четырех разных общих доменах, размещенных бесплатными поставщиками динамических DNS Duck DNS и FreeDNS :

kasperskylab.ignorelist.com

hpsj.firewall-gateway.net

googlechromeupdater.twilightparadox.com

iatassl-telechargementsecurity.duckdns.org

stub.ignorelist.com

Недостаточно доказательств для атрибуции

Используя инструменты с открытым исходным кодом для постэксплуатации и вредоносное ПО, которое широко используется в хакерских операциях несколькими участниками, LazyScripter оставляет мало подсказок относительно атрибуции.

Однако Malwarebytes отмечает, что публичные исследования показывают, что только два злоумышленника использовали инструмент тестирования на проникновение Koadic в своих кампаниях: связанный с Ираном MuddyWater и российский APT28 (Fancy Bear / Sofacy / Strontium / Sednit).

Компания заявляет, что не нашла связи с APT28, но заметила сходство с MuddyWater в том, что в их прошлых кампаниях использовались как Koadic, так и PowerShell Empire, и они полагались на GitHub для размещения своего вредоносного набора инструментов.

Однако есть некоторые аспекты, которые не допускают высоконадежной атрибуции и побудили Malwarebytes пометить LazyScripter как новую группу APT:

Кампании MuddyWater нацелены, в то время как LazyScripter's полагается на спам для охвата жертв

ни одно из вредоносных программ, используемых в кампаниях LazyScripter, в прошлом не было связано с MuddyWater

использование встроенных документов не характерно для MuddyWater, который обычно использует вредоносные макросы

использовались только широко доступные инструменты, в то время как MuddyWater также использует специальные инструменты в своих операциях.» ***(Ionut Ilascu. LazyScripter hackers target airlines with remote access Trojans // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/lazyscripter-hackers-target-airlines-with-remote-access-trojans/). 24.02.2021).***

***

Діяльність хакерів та хакерські угруповування

«Таинственная группа хактивистов в субботу отравила записи DNS нескольких веб-сайтов шри-ланкийцев (.lk) и перенаправила пользователей на веб-страницу, где подробно описаны различные социальные проблемы, влияющие на местное население.

Хотя большинство затронутых доменов были веб-сайтами местных предприятий и новостными сайтами, пострадали также два известных домена для Google.lk и Oracle.lk, сообщили ZDNet читатели в субботу.

Следующее сообщение было отображено на Google.lk в течение нескольких часов, прежде чем вмешались власти. В сообщении освещаются проблемы, связанные с местной чайной промышленностью, свободой прессы, предполагаемым коррумпированным политическим классом и судебной системой, а также проблемами расы, меньшинств и религии.

Это нападение произошло в субботу, 6 февраля, всего через два дня после официального дня национальной независимости Шри-Ланки, 4 февраля, что объясняет националистический посыл.

NIC.lk, администратор национального доменного пространства LK верхнего уровня страны, подтвердила атаку в субботу в сообщении, размещенном на ее веб-сайте.

«Проблема с системой регистрации доменов.LK возникла рано утром в субботу, 6 февраля, и затронула несколько доменов, зарегистрированных в.LK», - заявили в организации. «Этот вопрос был решен в срочном порядке, и вопрос был решен примерно к 8.30».

Комиссия по регулированию электросвязи Шри-Ланки также подтвердила инцидент в твите на своем аккаунте.

Подробности об атаке и количестве затронутых доменов не разглашаются. Представитель NIC.lk не ответил на запрос о комментарии, отправленный ZDNet в воскресенье.

Атака не осталась незамеченной в Шри-Ланке, и несколько пользователей написали об этом в Твиттере на выходных, даже если инцидент продолжался всего несколько часов.

Это второй инцидент, связанный с кибербезопасностью, который затронул организацию NIC.lk. В 2013 году хакеры использовали атаку с использованием SQL-инъекции, чтобы взломать базу данных и украсть данные о владельцах доменов.lk». ***(Catalin Cimpanu. Hacktivists deface multiple Sri Lankan domains, including Google.lk // ZDNet (https://www.zdnet.com/article/hacktivists-deface-multiple-sri-lankan-domains-including-google-lk/). 07.02.2021).***

***

«Исследователи раскрыли внутренние механизмы слежки хакерской группы «Domestic Kitten».

Domestic Kitten, также обозначаемый как APT-C-50, представляет собой группу повышенной постоянной угрозы (APT). APT, впервые обнаруженный в 2018 году, связан с иранским правительством и был связан с нападениями на местных граждан, «которые могут представлять угрозу стабильности иранского режима», согласно Check Point.

Целевые лица могут включать диссидентов режима, борцов за гражданские права, журналистов и юристов.

В сообщении в блоге в понедельник исследовательская группа Check Point сообщила, что Domestic Kitten в течение последних четырех лет проводил широкомасштабное наблюдение, запустив не менее 10 отдельных кампаний и поддерживая как минимум 1200 человек в целевом списке.

В настоящее время зарегистрировано четыре активных кампании, последняя из которых, похоже, началась в ноябре и продолжается. Жертвы домашних котят находятся по всему миру, в том числе в таких странах, как Иран, США, Пакистан и Турция.

APT использует мобильное вредоносное ПО FurBall. Вредоносная программа основана на коммерчески доступном программном обеспечении для мониторинга под названием KidLogger, и, по словам исследователей, «похоже, что разработчики либо получили исходный код KidLogger, либо перепроектировали образец и удалили все посторонние части, а затем добавили дополнительные возможности».

FurBall распространяется с помощью различных векторов атак, включая фишинг, иранские веб-сайты, каналы Telegram, а также посредством SMS-сообщений, содержащих ссылку на вредоносное ПО. Вредоносная программа использует различные маскировки, чтобы обманом заставить жертву выполнить установку; например, они упакованы как мобильная система безопасности «VIPRE», маскируются под новостное приложение, действуют как переупакованные законные мобильные игры, которые можно найти в Google Play, магазинах приложений, ресторанах и приложениях для обоев.

После установки на целевое устройство, FurBall может перехватывать SMS-сообщения, захватывать журналы вызовов, собирать информацию об устройстве, записывать сообщения, красть медиафайлы и сохраненные файлы, отслеживать координаты GPS устройства и, таким образом, отслеживать движения своих целей и многое другое.

Информация, собранная со взломанного устройства, может быть отправлена на серверы управления и контроля (C2), которые использовались компанией Domestic Kitten с 2018 года. Связанные IP-адреса были обнаружены в Иране, как в Тегеране, так и в Карадже.

В понедельник исследователи Check Point вместе с SafeBreach также раскрыли деятельность второй группы угроз, которая активно нацелена на иранских диссидентов - но вместо того, чтобы сосредоточиться на их смартфонах, их ПК подвергаются риску. Названный Infy, этот APT, который, как известно, существует с 2007 года и подозревается в том, что он спонсируется государством, теперь возобновил свои усилия, добавив ранее не обнаруженный штамм вредоносного ПО, обновленную основную полезную нагрузку вредоносного ПО Infy и капитальный ремонт предыдущей инфраструктуры C2». ***(Charlie Osborne. Domestic Kitten hacking group strikes local citizens considered a threat to Iranian regime // ZDNet (https://www.zdnet.com/article/domestic-kitten-hacking-group-strikes-local-citizens-considered-a-threat-to-iranian-regime/). 08.02.2021).***

***

«Группа антифашистских израильских хакеров взломала веб-сайт группы, связанной с сторонником превосходства белой расы Ку-клукс-кланом (KKK).

Впоследствии хакеры опубликовали в социальных сетях имена, фотографии и другую личную информацию о членах Патриотической бригады рыцарей, которую они скопировали.

Они также заменили часть содержимого сайта своим собственным.

Это включало плакат с надписью: «Шабат Шалом! Спокойной ночи, белая гордость».

Хакеры сообщили газете "Джерузалем пост", что они являются частью движения "Антифа", действующего под названием "Хаялим альмоним", что на иврите означает "анонимные солдаты".

И их целью было «вселить ужас в сердца врагов человечества».

Антифа - сокращение от антифашистского действия - движение, которое считается слабо организованной группой активистов без лидеров, выступает против неонацистов, фашизма, сторонников превосходства белой расы и расизма.

Среди информации, взятой с веб-сайта Patriotic Knight Brigade, было имя, номер телефона и адрес предполагаемого лидера группы.

'Террористическая деятельность'

Хаялим Алмоним также поделился ссылкой на Государственный реестр лиц, совершивших сексуальные преступления в Техасе, где, по его словам, старший член был зарегистрирован за сексуальное насилие над 14-летней девушкой.

«Впереди еще много всего», - сказал BBC News один из хакеров.

«Мы не собираемся останавливаться, пока не покончим с Кланом и не нанесем смертельный удар фашизму в Соединенных Штатах.

«Содействие фашистской террористической деятельности больше не будет терпимым».

Хакер добавил, что если другие антифашисты предпримут аналогичные действия, то «враги человечества задрожат от страха».

Ранее хакеры провели аналогичную атаку на Церковь Ку-клукс-клана, которая, по их словам, действовала в 25 штатах США». ***(Israeli hackers breach KKK-affiliated website // BBC (https://www.bbc.com/news/technology-55937133). 04.02.2021).***

***

«В четверг (18 февраля) хакеры атаковали правительственные сайты, управляемые хунтой в Бирме, в ответ на отключение Интернета, введенное властями четвертую ночь подряд. Группа, которая выдает себя за «Хакеры Бирмы», нацелилась на сайты Центрального банка, официальную страницу бирманской армии, сайт общественного телеканала MRTV, администрацию порта, а также сайт продовольственной и агентство по охране здоровья. «Мы боремся за справедливость в Бирме», - заявила хакерская группа на своей странице в Facebook. «Это похоже на массовую акцию протеста перед сайтами правительства», - сказал он.

Кибернаступление произошло после протестов, которые собрали десятки тысяч людей по всей стране в среду, чтобы выразить протест против военного переворота, в результате которого было свергнуто гражданское правительство Аунг Сан Су Чжи в начале этого месяца. Мэтт Уоррен, эксперт по кибербезопасности из австралийского университета RMIT в Мельбурне, сказал, что атака, по всей видимости, была направлена на повышение авторитета протестного движения. «Тип атак, в которых они участвуют, - это отказ в обслуживании или обезображивание сайтов, которые являются «хактивизмом», актами взлома, мотивированными активизмом, - сказал он AFP. «Воздействие потенциально ограничено, но это помогает предать гласности их причину».

Согласно NetBlocks, британской обсерватории по ограничению доступа в Интернет, еще одно отключение интернета было зафиксировано в 1 час ночи в четверг в Бирме. Интернет-соединение упало до 21% от их обычного уровня, сообщила обсерватория, в то время как докладчик ООН Том Эндрюс сказал, что

опасается роста насилия в среду после того, как ему сообщили об отправке солдат в Янгон». ***(Des hackers ciblent des sites gouvernementaux en Birmanie // Le Figaro (https://www.lefigaro.fr/flash-actu/des-hackers-ciblent-des-sites-gouvernementaux-en-birmanie-20210218). 18.02.2021).***

***

«Все больше хакерских групп, чем когда-либо прежде, нацелены на промышленные среды, поскольку кибератаки пытаются проникнуть в сети компаний, предоставляющих жизненно важные услуги, включая электроэнергию, воду, нефть и газ и производство.

К угрозам относятся киберпреступные группы, стремящиеся украсть информацию или зашифровать системы с помощью программ- вымогателей, а также хакерские операции при поддержке государства, пытающиеся определить потенциальные нарушения, которые они могут вызвать с помощью кибератак на операционные технологии (OT).

По данным исследователей кибербезопасности из Dragos, за последний год были обнаружены четыре новых хакерских группы, нацеленных на промышленные системы, и увеличился объем инвестиций со стороны кибер-злоумышленников, нацеленных на промышленность и системы промышленного управления.

Четыре новые группы, выявленные в течение прошлого года и названные исследователями как Stibnite, Talonite, Kamacite и Vanadinite, дополняют 11 ранее выявленных хакерских групп, нацеленных на системы промышленного контроля.

У некоторых из этих новых групп есть очень конкретные цели - например, Stibnite фокусируется на компаниях, производящих ветряные турбины, которые вырабатывают электроэнергию в Азербайджане, а Talonite почти исключительно сосредотачивается на попытке получить доступ к поставщикам электроэнергии в США.

Остальные новые хакерские группы имеют более общие цели; Камасит, который Драгос связывает с группой Sandworm, нацелен на промышленные операции энергетических компаний в Северной Америке и Европе.

Тем временем Vanadinite проводит операции против энергетики, производства и транспорта в Северной Америке, Европе, Австралии и Азии, уделяя особое внимание сбору информации и компрометации АСУ ТП.

Обнаружение четырех дополнительных операций взлома, нацеленных на промышленные системы, действительно вызывает беспокойство, но их обнаружение также указывает на то, что угрозы для промышленных систем становятся все более заметными. Эти угрозы могли быть упущены в предыдущие годы.

«Чем больше мы видим в пространстве OT, тем лучше понимаем его ландшафт угроз и активных противников, которых мы можем идентифицировать», - сказал ZDNet Серджио Кальтаджироне, вице-президент по анализу угроз Dragos.

«Сетевые атаки OT требуют иного подхода, чем традиционная ИТ-безопасность. ИТ-инциденты имеют высокую частоту и относительно малозатратные инциденты и последствия по сравнению с OT-атаками, которые менее часты, но потенциально имеют очень высокие воздействия и эффекты».

Однако, согласно исследованию, видимость остается проблемой для промышленных сетей, поскольку 90% организаций, исследованных Драгосом, не имеют полного представления о своей собственной сети ОТ, что может помочь кибер-злоумышленникам остаться незамеченными.

Во многих случаях хакеры могут сочетать отсутствие видимости со способностью прятаться у всех на виду, злоупотребляя законными учетными данными, чтобы помочь перемещаться по сети.

Часто кампании, нацеленные на промышленные системы, включают фишинговые атаки или использование удаленных сервисов, позволяя злоумышленникам использовать реальные учетные записи для выполнения злонамеренных действий, одновременно помогая избежать обнаружения подозрительных.

«Отсутствие видимости значительно увеличивает риски, потому что дает противнику свободу проводить операции беспрепятственно, время, чтобы понять среду жертвы, определить свои цели, достичь желаемых результатов и удовлетворить намерение по достижению компромисса», - сказал Кальтаджироне.

Эта деятельность может иметь физические эффекты вне сетевой среды, как недавно было продемонстрировано, когда злоумышленник смог изменить химические свойства питьевой воды после взлома сети водоочистного сооружения в городе Олдсмар, штат Флорида.

Есть также примеры, когда кибер-злоумышленники получали доступ к электросетям до такой степени, что они могли отключить электричество.

SEE: Фишинг: это наиболее распространенные методы, используемые для атаки на ваш компьютер.

Однако существуют процедуры кибербезопасности, которые промышленные организации могут предпринять, чтобы повысить видимость своих собственных сетей и помочь защитить системы от кибер-вторжений.

К ним относятся определение того, какие активы осуществляют контроль над критически важными операциями, и определение приоритетов безопасности, чтобы помочь злоумышленникам получить к ним более сложный доступ, а также настройка процедур, облегчающих выявление атак.

Организациям также следует попытаться применить сегментацию сети, отделяя операционные технологии от информационных технологий, чтобы в случае взлома ИТ-сети злоумышленниками было непросто перейти к элементам управления ОТ в той же сети.

Учетные данные для входа также должны быть должным образом защищены с помощью многофакторной проверки подлинности, в то время как организациям следует избегать использования учетных данных по умолчанию, чтобы обеспечить дополнительные барьеры для удаленных злоумышленников». ***(Danny Palmer. These four new hacking groups are targeting critical infrastructure, warns security company // ZDNet (https://www.zdnet.com/article/these-four-new-hacking-groups-are-targeting-critical-infrastructure-warns-security-company/). 25.02.2021).***

***

«Китайские хакеры, спонсируемые государством, преследовали тибетские организации по всему миру, используя вредоносную надстройку Firefox, которая была настроена для кражи данных браузеров Gmail и Firefox с последующей загрузкой вредоносных программ в зараженные системы.

Атаки, обнаруженные в этом месяце фирмой Proofpoint, занимающейся кибербезопасностью, были связаны с группой, которую компания отслеживает под кодовым названием TA413.

БЫЛИ НАЦЕЛЕНЫ ТОЛЬКО НА ПОЛЬЗОВАТЕЛЕЙ FIREFOX

Proofpoint заявил, что злоумышленники нацелились на тибетские организации с помощью целевых фишинговых писем, которые заманивали участников на веб-сайты, где им предлагалось установить обновление Flash для просмотра содержимого сайта.

Эти веб-сайты содержали код, разделяющий пользователей. Только пользователям Firefox с активным сеансом Gmail предлагалось установить вредоносное дополнение.

Команда Proofpoint заявила, что, хотя расширение было названо «Компоненты обновления Flash», на самом деле оно было версией законной надстройки «Уведомление Gmail (без перезапуска)» с дополнительным вредоносным кодом. По мнению исследовательской группы, этот код может злоупотреблять следующими функциями в зараженных браузерах:

Gmail:

Искать электронные письма

Архивировать электронные письма

Получать уведомления Gmail

Читать электронные письма

Изменение функций звуковых и визуальных предупреждений в браузере Firefox

Пометить электронные письма

Помечает электронные письма как спам

Удалить сообщения

Обновить папку "Входящие"

Пересылка писем

Выполните поиск функций

Удалять сообщения из корзины Gmail

Отправлять почту со взломанного аккаунта

Firefox (на основе предоставленных разрешений браузера):

Доступ к пользовательским данным для всех сайтов

Отображать уведомления

Читать и изменять настройки конфиденциальности

Доступ к вкладкам браузера

Но атака на этом не закончилась. Proofpoint сообщил, что расширение также загружало и устанавливало вредоносное ПО ScanBox в зараженных системах.

Эта вредоносная программа, основанная на PHP и JavaScript, представляет собой старый инструмент, использованный в предыдущих атаках, осуществленных китайскими кибершпионажными группами.

«С 2014 года Scanbox использовался в многочисленных кампаниях, направленных на тибетскую диаспору и другие этнические меньшинства, которые часто становятся мишенью групп, поддерживающих интересы китайского государства», - говорится в сегодняшнем докладе Proofpoint.

Последний зарегистрированный случай атаки ScanBox датируется 2019 годом, когда Recorded Future сообщила об атаках на посетителей пакистанских и тибетских веб-сайтов.

Что касается своих возможностей, Proofpoint утверждает, что ScanBox «способен отслеживать посетителей определенных веб-сайтов, выполнять кейлоггеры и собирать пользовательские данные, которые могут быть использованы в будущих попытках вторжения», что делает установку этой опасной угрозы в ваших системах.

FLASH EOL МОГ ПОМОЧЬ ЗЛОУМЫШЛЕННИКАМ

В этой конкретной кампании, которую Proofpoint назвал FriarFox, атаки начались в январе 2021 года и продолжались в течение февраля.

Хотя хакеры годами использовали поддельные темы обновлений Flash, и большинство пользователей знают, что им следует держаться подальше от веб-сайтов, предлагающих обновления Flash совершенно неожиданно, считается, что эти атаки сработали намного лучше, чем предыдущие.

Причина в том, что Adobe удалила Flash Player в конце 2020 года, а весь Flash-контент перестал воспроизводиться в браузерах 12 января 2021 года, когда Proofpoint также увидел первые кампании TA413 FriarFox, нацеленные на тибетские организации». ***(Catalin Cimpanu. Chinese cyberspies targeted Tibetans with a malicious Firefox add-on // ZDNet (https://www.zdnet.com/article/chinese-cyberspies-targeted-tibetans-with-a-malicious-firefox-add-on/). 25.02.2021).***

***

«Киберпреступные хакерские операции теперь настолько квалифицированы, что национальные государства используют их для проведения атак, пытаясь скрыть свое собственное участие.

В отчете исследователей кибербезопасности BlackBerry содержится предупреждение о том, что появление сложных схем «киберпреступность как услуга» означает, что национальные государства все чаще имеют возможность работать с группами, которые могут проводить за них атаки.

Эта киберпреступная операция обеспечивает злонамеренные хакерские операции, такие как фишинг, вредоносное ПО или взлом сетей, и получает деньги за свои действия, в то время как национальное государство, заказавшее операцию, получает информацию или доступ, который ему требуется.

Это также дает дополнительный бонус: поскольку атака была проведена киберпреступниками, которые использовали свою собственную инфраструктуру и методы, трудно связать эту деятельность с национальным государством, которое заказало операцию.

«Появление, изощренность и анонимность криминального ПО как услуги означает, что государства могут маскировать свои усилия сторонними

подрядчиками и почти непреодолимой стеной правдоподобного отрицания», - предупреждает BlackBery 2021 Threat Report.

Исследователи указывают на существование обширных хакерских операций, таких как Bahamut, в качестве примера того, насколько изощренными стали киберпреступные кампании.

Первоначально описанный BlackBerry в прошлом году, Бахамут использует фишинг, социальную инженерию, вредоносные приложения, нестандартные вредоносные программы и атаки нулевого дня в кампаниях, нацеленных на правительства, частный сектор и отдельных лиц по всему миру - и делал это в течение многих лет, прежде чем был обнаружен.

Исследователи отмечают, что «профили и география их жертв слишком разнообразны, чтобы соответствовать интересам одного злоумышленника», предполагая, что Бахамут выполняет операции для разных клиентов, следя за работой, которая принесет им больше всего денег. Что касается финансирования, то у некоторых национальных государств больше всего денег, которые они могут потратить на проведение кампаний.

Мало того, что клиентское национальное государство в конечном итоге получает требуемый доступ к взломанным сетям или конфиденциальной информации, это позволяет сделать это с меньшими шансами на его обратную связь с национальным государством - а это означает, что это потенциально позволит избежать последствий или осуждения. для проведения атак.

«Идентификация злоумышленников может быть сложной задачей для исследователей угроз из-за нескольких факторов, таких как перекрывающаяся инфраструктура, несопоставимые цели и необычная тактика. Это особенно верно, когда только часть кампании передается на аутсорсинг», - говорится в отчете.

Бахамут продолжал проявлять активность с момента его первоначального раскрытия в прошлом году, проводя кампании, нацеленные на правительственные учреждения, связанные с иностранными делами и обороной на Ближнем Востоке. Группа также проводит кампании против целей в Южной Азии, уделяя особое внимание атакам со смартфонов.

Хотя защита сетей от решительных кибератак может быть сложной, существуют методы кибербезопасности, которые организации могут применять для предотвращения вторжений, например, предоставление удаленного доступа к конфиденциальной информации только тем, кто в ней абсолютно нуждается, и постоянное изучение сети на предмет необычной активности, которая может было бы классифицировано как подозрительное». ***(Danny Palmer. Cybercrime groups are selling their hacking skills. Some countries are buying // ZDNet (https://www.zdnet.com/article/cybercrime-groups-are-selling-their-hacking-skills-some-countries-are-buying/). 26.02.2021).***

***

«Поддерживаемая Северной Кореей хакерская группа с начала 2020 года нацелена на оборонную промышленность с помощью специального вредоносного ПО для бэкдора, получившего название ThreatNeedle, с конечной целью сбора очень конфиденциальной информации.

Эта шпионская кампания затронула организации из более чем десятка стран и координировалась поддерживаемыми КНДР государственными хакерами, известными как Lazarus Group.

В качестве исходного вектора доступа к корпоративной сети компании злоумышленники использовали целевые фишинговые письма на тему COVID19 с вредоносными вложениями или ссылками.

После первоначального взлома они установили специально разработанное группой вредоносное ПО ThreatNeedle для бэкдора, которое впервые использовалось в 2018 году в атаках, направленных на криптовалютные компании.

«После установки ThreatNeedle может получить полный контроль над устройством жертвы, то есть он может делать все, от манипулирования файлами до выполнения полученных команд», - заявили сегодня исследователи Kaspersky Security.

ThreatNeedle помог хакерам Lazarus перемещаться по сетям оборонных организаций и собирать конфиденциальную информацию, которая передавалась на контролируемые злоумышленником серверы с помощью специального инструмента туннелирования через туннели SSH на удаленные скомпрометированные южнокорейские серверы.

Бэкдор также позволил им обойти сегментацию сети и получить доступ к сетям с ограниченным доступом с помощью критически важных устройств, не имеющих доступа в Интернет.

«После того, как злоумышленники закрепились на начальном этапе, злоумышленники собрали учетные данные и двинулись в сторону, ища важные активы в среде жертвы», - добавил Касперский.

«Мы наблюдали, как они преодолели сегментацию сети, получив доступ к машине с внутренним маршрутизатором и настроив ее в качестве прокси-сервера, что позволило им пересылать украденные данные из интрасети на их удаленный сервер».

Во время своих атак хакеры также были замечены во воровстве документов и данных как из офисных ИТ-сетей (с устройств, используемых для хранения информации о бизнесе и клиентах), так и из сетей с ограниченным доступом (обычно используемых для хранения и управления высокочувствительными данными).

Операторы Lazarus взяли под свой контроль рабочие станции администраторов, что позже позволило им установить вредоносные шлюзы, которые предоставили им доступ к ограниченным сетям.

В то время как Lazarus Group была известна тем, что сосредоточила свои усилия в основном на нацеливании на мировые финансовые учреждения, начиная с начала 2020 года, когда началась эта кампания, они переключили свое внимание на «агрессивные атаки» на организации оборонной промышленности.

После этого шага хакеры Lazarus перепрофилировали свое вредоносное ПО ThreatNeedle для кражи конфиденциальной информации в рамках целевых шпионских атак.

«Lazarus был, пожалуй, самым активным злоумышленником в 2020 году, и не похоже, что это изменится в ближайшее время», - сказал старший исследователь Kaspersky GReAT по безопасности Сонсу Пак.

«Фактически, уже в январе этого года группа анализа угроз Google сообщила, что Lazarus использовала тот же бэкдор для нацеливания на исследователей безопасности. Мы ожидаем увидеть больше ThreatNeedle в будущем, и мы будем следить за этим. "

Хакеры Lazarus также отслеживаются разведывательным сообществом США как HIDDEN COBRA).

Это хорошо известная финансово мотивированная группа киберпреступников, о чем свидетельствуют их кампании: они взломали Sony Films в рамках операции Blockbuster в 2014 году и стояли за глобальной кампанией по вымогательству WannaCry в 2017 году». ***(Sergiu Gatlan. North Korean hackers target defense industry with custom malware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/north-korean-hackers-target-defense-industry-with-custom-malware/). 25.02.2021).***

***

«Хакерская группа под названием Hotarus Corp взломала Министерство финансов Эквадора и крупнейший банк страны Banco Pichincha, где они утверждают, что украли внутренние данные.

Вначале банда вымогателей нацелилась на Министерство финансов Эквадора, Ministerio de Economía y Finanzas de Ecuador, где они развернули программу-вымогатель на основе PHP для шифрования сайта, на котором размещен онлайн-курс.

Исследователь безопасности Херман Фернандес сообщил BleepingComputer, что злоумышленники используют обычную программу- вымогатель PHP под названием Ronggolawe (или AwesomeWare) для шифрования содержимого сайта.

Вскоре после атаки злоумышленники опубликовали на хакерском форуме текстовый файл, содержащий 6632 имени входа и хешированные комбинации паролей.

Банда вымогателей сообщила BleepingComputer, что они украли «секретную министерскую информацию, электронные письма, информацию о сотрудниках, контракты».

Целевой Banco Pichincha следующий

После атаки Министерства финансов Hotarus Corp взломала крупнейший частный банк Эквадора Banco Pichincha.

Банк подтвердил атаку в официальном заявлении, но заявляет, что это был взломанный маркетинговый партнер, а не его внутренние системы.

Banco Pichincha сообщает, что злоумышленники использовали взломанную платформу для рассылки фишинговых писем клиентам, пытаясь украсть конфиденциальную информацию для выполнения «незаконных транзакций».

С полным переводом выписки банка можно ознакомиться ниже.

«Мы стремимся защищать конфиденциальность данных наших клиентов. Мы знаем, что имел место несанкционированный доступ к системам поставщика,

который предоставляет маркетинговые услуги для программы Pichincha Miles. В отношении этой утечки информации и на основе обширного расследования, мы не обнаружили доказательств повреждения или доступа к системам Банка, и, следовательно, безопасность финансовых ресурсов наших клиентов не подвергается риску.

Мы знаем, что через мошенническое электронное письмо злоумышленник отправляет сообщения от имени Banco Pichincha некоторым клиентам указанной программы, чтобы получить информацию, необходимую для выполнения незаконных транзакций. Мы напоминаем нашим клиентам, что мы никогда не запрашиваем конфиденциальные данные, такие как: пользователи, пароли, данные карты или учетной записи, по телефону, электронной почте, в социальных сетях или текстовых сообщениях.

Мы принимаем меры для предотвращения и смягчения подобных ситуаций, связанных с обработкой данных нашими поставщиками. Мы понимаем и разделяем озабоченность людей, чья информация была раскрыта, и подтверждаем нашу приверженность их безопасности», - Banco Pichincha

В интервью BleepingComputer группа хакеров оспаривает заявление банка и заявляет, что они использовали атаку маркетинговой компании в качестве стартовой площадки для внутренних систем банка. Затем они украли данные и использовали программы-вымогатели для шифрования устройств.

"Взгляните на атаку на банк, первоначально на компанию, которая разрабатывает веб-приложения и занимается маркетингом для банка. После анализа кодов и данных она дала нам возможность получить доступ к внутренним системам банка, именно там мы использовали программу-вымогатель, извлекая все возможная информация».

«Оказавшись внутри, мы обнаружили уязвимости в их приложениях, эксплойты в портах ftp и rdp, которые помогли нам повысить привилегии», - сказали BleepingComputer злоумышленники.

В ходе этой атаки хакерская группа утверждает, что похитила «31 636 026 миллионов записей о клиентах и 58 456 конфиденциальных системных записей», включая номера кредитных карт.

В качестве доказательства своей атаки хакерская группа предоставила различные изображения якобы украденных данных, включая следующую папку с файлами.

BleepingComputer не смог проверить утверждения злоумышленников о краже данных из Министерства финансов или Banco Pichincha.

В этом за деньги

Злоумышленники сообщили BleepingComputer, что проводят эти атаки исключительно ради денег.

Они заявляют, что в настоящее время не продают данные, украденные у Министерства финансов, а продают кредитные карты, которые, по их утверждениям, были украдены у Banco Pichincha.

«В настоящее время продается только банковская информация, мы уже продали около 37 тысяч кредитных карт группе, занимающейся этим, информация

будет продана на аукционе или продана первоначально за 250 тысяч», - сообщил BleepingComputer оператор Hotarus Corp.

Мы связались с Министерством финансов Эквадора и Banco Pichincha, чтобы узнать больше об атаках, но на данный момент не получили ответа». ***(Lawrence Abrams. Ransomware gang hacks Ecuador's largest private bank, Ministry of Finance // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ransomware-gang-hacks-ecuadors-largest-private-bank-ministry-of-finance/). 26.02.2021).***

***

«В середине 2020 года эксперты «Лаборатории Касперского» обнаружили новую вредоносную кампаниюAPT-группы Lazarus. Злоумышленники расширили своё портфолио атаками на оборонную промышленность, в которых они использовали вредоносное ПО ThreatNeedle, относящееся к кластеру Manuscrypt. В результате атакующим удалось преодолеть сегментацию сети и получить доступ к конфиденциальной информации. Среди жертв атак были предприятия из России. Также были зарегистрированы обращения к инфраструктуре злоумышленников из Европы, Северной Америки, Ближнего Востока и Азии, что может говорить о возможных жертвах и в этих регионах.

Lazarus ведёт свою деятельность как минимум с 2009 года, организуя широкомасштабные кампании кибершпионажа, операции с применением программ-шифровальщиков и даже атаки на криптовалютный рынок. В последние годы группа была сосредоточена на атаках на финансовые учреждения по всему миру. Однако с начала 2020 года среди целей злоумышленников оказались и предприятия оборонной промышленности.

«Лаборатория Касперского» получила возможность более детально исследовать атаку, когда одна из пострадавших организаций обратилась за помощью. Эксперты компании обнаружили в сети бэкдор ThreatNeedle, ранее замеченный в атаках Lazarus на криптовалютные компании.

Начальное заражение происходило путём целевого фишинга: злоумышленники направляли письма с вредоносными документами Microsoft Word или ссылками на такие документы, размещённые на удаленном сервере. Злоумышленники сделали ставку на актуальную тему — профилактику и диагностику коронавирусной инфекции. Письма были написаны якобы от имени сотрудника медицинского центра, входящего в состав атакованной организации.

Если пользователь открывал вредоносный документ и разрешал выполнение макросов, зловред переходил к многоэтапной процедуре развёртывания. После установки ThreatNeedle злоумышленники получали практически полный контроль над устройством.

Одна из наиболее интересных деталей данной кампании связана с тем, как злоумышленники преодолели сегментацию сети. Сеть атакованного предприятия была разделена на два сегмента: корпоративный (сеть, компьютеры которой имеют доступ к интернету) и изолированный (сеть, компьютеры которой содержат конфиденциальные данные и не имеют доступа к интернету). При этом, согласно политикам безопасности, любая передача информации между этими сегментами

запрещена, то есть они должны быть полностью разделены. Однако на деле администраторы имели возможность подключения к обоим сегментам для настройки и оказания технической поддержки пользователям в обеих зонах. Злоумышленникам удалось получить учётные данные от маршрутизатора, используемого администраторами для подключений к изолированной и корпоративной сетям. Изменив его настройки и установив на нём дополнительное ПО, они смогли превратить его в хостинг вредоносного ПО в сети предприятия. После этого маршрутизатор использовался для проникновения в изолированный сегмент, вывода данных из него и отправки их на командный сервер.

«Lazarus была, возможно, самой активной кибергруппой в 2020 году и, похоже, остаётся таковой. В январе 2021 года команда анализа угроз Google Threat Analysis Team сообщила, что Lazarus использует тот же бэкдор для атак на исследователей в области кибербезопасности. Мы полагаем, что неоднократно увидимThreatNeedle в будущем, и продолжим следить за этим бэкдором», — комментирует Сеонгсу Парк (Seongsu Park), старший эксперт команды GReAT.

«Lazarus — не только сверхактивная группа, но и весьма продвинутая. Злоумышленники не только преодолели сегментацию сети, но и провели тщательное исследование, чтобы создать персонализированную и эффективную фишинговую рассылку и кастомизированные инструменты для передачи украденной информации на удалённый сервер. Предприятиям необходимо принимать дополнительные меры безопасности для защиты от такого рода кампаний кибершпионажа», — добавляет Вячеслав Копейцев, старший эксперт Kaspersky ICS CERT.

Чтобы защитить организацию от подобных кибератак, «Лаборатория Касперского» рекомендует компаниям регулярно проводить для сотрудников тренинги по кибербезопасности, поскольку целевые атаки часто начинаются с фишинга или других техник социальной инженерии; если на предприятии есть сегменты сети, которые должны быть изолированы от прочих сетей и интернета, регулярно проверять, так ли это на самом деле, например при помощи периодическиханализов защищённости и тестов на проникновение; дополнительно рекомендуем установить и использовать средства мониторинга сетевой активности внутри и на границе периметра изолированной сети; удостовериться, что сотрудники ознакомлены с политиками кибербезопасности и следуют им; предоставить специалистам SOC-центра доступ к самым свежим данным об угрозах, например к порталу Kaspersky Threat Intelligence Portal, на котором собраны данные о кибератаках, накопленные за более 20 лет работы «Лаборатории Касперского», включая информацию об угрозах промышленным организациям и системам промышленной автоматизации». ***(Владимир Бахур. «Лаборатория Касперского»: Lazarus атакует оборонные предприятия по всему миру // CNews (https://safe.cnews.ru/news/line/2021-02-25_laboratoriya_kasperskogo). 25.02.2021).***

***

«Вариант троянца Masslogger используется в атаках, направленных на кражу учетных данных учетных записей Microsoft Outlook, Google Chrome и служб обмена сообщениями.

В среду исследователи кибербезопасности из Cisco Talos заявили, что кампания в настоящее время ориентирована на жертв в Турции, Латвии и Италии, расширяя деятельность, задокументированную в конце 2020 года, которая нацелена на пользователей в Испании, Болгарии, Литве, Венгрии, Эстонии и Румынии.

Похоже, что цели меняются почти ежемесячно.

Впервые Masslogger был замечен в дикой природе в апреле 2020 года в соответствии с лицензионными соглашениями, согласованными на подпольных форумах. Тем не менее, новый вариант считается «примечательным» Talos из-за использования скомпилированного формата файла HTML для запуска цепочки заражения.

Злоумышленники начинают свои атаки обычным способом - с помощью фишинговых писем. В этой волне атак фишинговые сообщения маскируются под бизнес-запросы и содержат вложения.RAR.

Если жертва открывает вложение, они разбиваются на многотомные архивы с расширением «r00», что, по мнению исследователей, может быть попыткой «обойти любые программы, которые блокируют вложение электронной почты на основе расширения файла. "

Затем извлекается скомпилированный HTML-файл.CHM - формат по умолчанию для законных файлов справки Windows, который содержит дополнительный HTML-файл со встроенным кодом JavaScript. На каждом этапе код обфусцируется и в конечном итоге приводит к развертыванию сценария PowerShell, который содержит загрузчик Masslogger.

Вариант троянца Masslogger, разработанный для компьютеров с Windows и написанный на.NET, затем начнет кражу учетных данных пользователя и не придирчив к своим целям - риску подвергаются как домашние пользователи, так и предприятия, хотя, похоже, операторы сосредотачиваются на последний.

После сохранения в памяти в виде буфера, сжатого с помощью gzip, вредоносная программа начинает сбор учетных данных. Microsoft Outlook, Google Chrome, Firefox, Edge, NordVPN, FileZilla и Thunderbird входят в число приложений, на которые нацелен троян.

Похищенная информация может быть отправлена по каналам SMTP, FTP или HTTP. Информация, загружаемая на сервер эксфильтрации, включает имя пользователя ПК жертвы, идентификатор страны, идентификатор компьютера и временную метку, а также записи, касающиеся параметров конфигурации и запущенных процессов.

«Наблюдаемая кампания почти полностью выполняется и присутствует только в памяти, что подчеркивает важность проведения регулярного и фонового сканирования памяти», - говорит Талос. «Единственный компонент на диске - это вложение и скомпилированный HTML-файл справки».

Исследователи отмечают, что Masslogger также может действовать как кейлоггер, но в этом варианте, похоже, функция кейлоггера была отключена.

Cisco Talos считает, что на основе индикаторов компрометации (IoC) кибератаки также могут быть связаны с прошлым использованием троянов AgentTesla, Formbook и AsyncRAT». ***(Charlie Osborne. Masslogger Trojan reinvented in quest to steal Outlook, Chrome credentials // ZDNet (https://www.zdnet.com/article/masslogger-trojan-reinvented-to-steal-outlook-chrome-credentials/). 18.02.2021).***

***

«Владельцы популярного приложения для сканирования штрих-кода, которое с помощью одного обновления стало вредоносным для миллионов устройств, настаивают на том, что виноват сторонний покупатель.

Ранее в этом месяце компания Malwarebytes, занимающаяся кибербезопасностью, исследовала, как надежное и полезное приложение для сканирования штрих-кодов и QR-кодов в Google Play, на которое было установлено более 10 миллионов установок, стало вредоносным в мгновение ока.

В последние месяцы пользователи начали жаловаться на то, что их мобильные устройства внезапно наполнились нежелательной рекламой, завоевав поклонников и долгие годы действуя как невинное программное обеспечение.

Сканер штрих-кода был назван виновником и источником вредоносного ПО, отслеживаемым как Android / Trojan.HiddenAds.AdQR. Исследователи отследили вредоносные обновления как причину - с агрессивным продвижением рекламы, реализованным в коде приложения.

Код аналитики приложения также был изменен, и обновления были сильно запутаны.

Malwarebytes сказал, что владелец, Lavabird Ltd., скорее всего, был виноват из-за регистрации собственности на момент обновления. Как только сообщили, программное обеспечение было извлечено из Google Play.

В то время Lavabird не ответила на запросы о комментариях. Однако поставщик теперь обратился к Malwarebytes с объяснением ситуации.

12 февраля Malwarebytes заявил, что Lavabird обвинил учетную запись под названием «космическая команда» в изменениях, произошедших после сделки о покупке, в результате которой право собственности на приложение переходит из рук в руки.

Lavabird приобрела сканер штрих-кода 23 ноября, и последующая сделка с космической командой была согласована 25 ноября.

Хотя исследовательская группа не смогла связаться с «космической командой», Lavabird сказал Malwarebytes 10 февраля, что они «не меньше возмущены», и Lavabird действовал только как «посредник» между «продавцом и покупателем в этой ситуации». "

По словам Lavabird, компания разрабатывает, продает и покупает мобильные приложения. В этом случае компания настаивает на том, чтобы космическая команда, покупающая сканер штрих-кода, получила доступ к консоли Google Play

приложения для проверки ключа и пароля программного обеспечения перед покупкой.

По словам Лаваберд, именно покупатель отправил вредоносное обновление пользователям сканера штрих-кода.

«Передача ключа подписи приложения при передаче права собственности на приложение является законной частью [процесса]», - комментируют исследователи. «Таким образом, запрос «космической команды» проверить работоспособность закрытого ключа путем загрузки обновления в Google Play кажется правдоподобным».

После выполнения обновления 7 декабря приложение было перенесено в учетную запись покупателя в Google Play. Однако Malwarebytes сообщает, что на момент обновления вредоносного ПО право собственности все еще принадлежало Lavabird.

Первое вредоносное обновление произошло 27 ноября, а последующие обновления скрывали код вредоносного ПО до 5 января, прежде чем приложение было не опубликовано.

Lavabird не проверила покупателя, выяснив его «молва». Однако в компании заявили, что «этот урок останется с нами на всю жизнь».

«Судя по моему анализу, то, что, по-видимому, произошло, - это хитрый подвиг социальной инженерии, в ходе которого разработчики вредоносных программ купили уже популярное приложение и использовали его», - прокомментировал исследователь Malwarebytes Натан Коллиер. «При этом они смогли взять приложение с 10 миллионами установок и превратить его в вредоносное ПО. Даже если часть этих установок обновляет приложение, это уже много заражений. И, имея возможность изменять код приложения раньше полная покупка и передача, они смогли проверить, не обнаружено ли их вредоносное ПО в аккаунте другой компании Google Play».

Если это правда, и это утверждение принято Коллиером, этот случай указывает на интересный способ для злоумышленников использовать разработчиков приложений, трейдеров и тестировать обнаружение вредоносных программ в Google Play через установленные и надежные базы пользователей.

«Нам очень жаль, что приложение стало вирусом, для нас это не только удар по нашей репутации», - сказал Лаваберд Malwarebytes. «Мы надеемся, что пользователи удалят приложение с вирусом со своих телефонов». ***(Charlie Osborne. Owner of app that hijacked millions of devices with one update exposes buy-to-infect scam // ZDNet (https://www.zdnet.com/article/owner-of-app-that-hijacked-millions-of-devices-with-one-update-exposes-buy-to-infect-scheme/). 17.02.2021).***

***

«Были обнаружены два варианта шпионского ПО для Android, связанные с проиндийскими хакерскими кампаниями, спонсируемыми государством.

Во вторник компания Lookout, занимающаяся кибербезопасностью, сообщила, что два штамма вредоносных программ, получившие название Hornbill и

SunBird, были связаны с Confucius, группой продвинутых постоянных угроз (APT), которая, как считается, спонсируется государством и имеет проиндийские связи.

Конфуций, впервые обнаруженный в 2013 году, был связан с нападениями на правительственные учреждения в Юго-Восточной Азии, а также с целенаправленными ударами по пакистанским военным, индийским избирательным органам и ядерным агентствам.

По данным фирмы, занимающейся кибербезопасностью, APT может быть разумно связан с Hornbill и SunBird, двумя формами шпионского ПО для Android. В частности, вредоносное ПО, по-видимому, нацелено на взлом платформы обмена сообщениями WhatsApp и извлечение содержимого разговоров.

Анализ вредоносного ПО, проведенный командой, предполагает, что Hornbill основан на MobileSpy, коммерческом приложении-преследователе для удаленного мониторинга устройств Android, которое было выведено из эксплуатации в 2018 году. SunBird, однако, имеет кодовую базу, аналогичную BuzzOut, старой форме шпионского ПО, разработанной в Индии.

Было известно, что Confucius использовал ChatSpy для наблюдения еще в 2017 году, но считается, что SunBird появился раньше этого вредоносного ПО. Похоже, что не будет никаких новых кампаний с использованием SunBird, которые, как полагают, активно разрабатывались с 2016 по начало 2019 года; Тем не менее, Hornbill был обнаружен в ходе волны атак, начиная с декабря 2020 года.

Апурва Кумар, инженер службы безопасности Lookout, говорит, что обе формы шпионского ПО используют службы специальных возможностей Android для хищения информации в Whatsapp и эксфильтрации контента без необходимости root-доступа или взломанного устройства.

Мобильные приложения, содержащие вредоносное ПО, по-видимому, размещаются за пределами Google Play и предлагаются в виде пакетов программного обеспечения, включая поддельную «Google Security Framework», агрегаторы местных новостей, приложения, связанные с исламом, и спортивное программное обеспечение. По данным Lookout, большинство этих вредоносных приложений нацелены на мусульманское население.

У Hornbill и SunBird разные подходы к шпионажу. Hornbill описывается как «инструмент скрытого наблюдения», предназначенный для выборочной кражи данных, представляющих интерес для его оператора, тогда как SunBird содержит функцию трояна удаленного доступа (RAT), позволяющую дополнительное развертывание вредоносных программ и удаленный захват.

Однако оба варианта вредоносного ПО могут красть данные, включая идентификаторы устройств, журналы вызовов, голосовые заметки WhatsApp, списки контактов и информацию о местоположении GPS. Кроме того, они могут запрашивать права администратора на взломанном устройстве, делать снимки экрана и фотографии, а также записывать звук как во время звонков, так и просто в качестве шума окружающей среды.

Возможности SunBird выходят за рамки возможностей Hornbill, поскольку это вредоносное ПО также может захватывать историю браузера, информацию календаря, контент BlackBerry Messenger (BBM) и более обширный контент WhatsApp, включая документы, базы данных и изображения. SunBird также будет

пытаться загружать украденные данные на сервер управления и контроля (C2) с более регулярными интервалами, чем Hornbill.

Однако Hornbill может обнаруживать и записывать активные звонки в WhatsApp, злоупотребляя функциями доступности Android.

«Использование служб доступности Android таким образом - это тенденция, которую мы часто наблюдаем в программном обеспечении Android для наблюдения, что позволяет избежать необходимости повышения привилегий на устройстве», - говорят исследователи». **(Charlie Osborne. Android spyware strains linked to state-sponsored Confucius threat group // ZDNet (https://www.zdnet.com/article/new-novel-android-spyware-linked-to-pro-india-confucius-threat-group/). 11.02.2021).**

***

«Microsoft заявляет, что количество вредоносных веб-оболочек, установленных на веб-серверах, почти удвоилось с момента последнего подсчета в августе 2020 года.

Вчера в блоге компания Redmond сообщила, что в период с августа 2020 года по январь 2021 года обнаруживала примерно 140000 веб-оболочек в месяц, по сравнению со средним показателем в 77000, который сообщалось в прошлом году.

Это число увеличилось в результате изменения взглядов хакеров на веб-оболочки. Когда-то считавшиеся инструментом для скриптовых детишек, дезориентирующих веб-сайты, и инструментом операторов бот-сетей DDoS, веб-оболочки теперь являются частью арсенала банд программ-вымогателей и хакеров национальных государств и являются важнейшими инструментами, используемыми в сложных вторжениях.

Две из причин, по которым они стали такими популярными, - это их универсальность и доступ к взломанным серверам.

Веб-оболочки, которые представляют собой не что иное, как простые сценарии, могут быть написаны практически на любом языке программирования, который работает на веб-сервере, например, PHP, ASP, JSP или JS, и т. Д. И могут быть легко спрятаны внутри исходного кода веб-сайта. Это делает их обнаружение сложной операцией, которая часто требует ручного анализа, выполняемого человеком-оператором.

Кроме того, веб-оболочки предоставляют хакерам простой способ выполнять команды на взломанном сервере через графический интерфейс или интерфейс командной строки, предоставляя злоумышленникам простой способ эскалации атак.

ВЕБ-ОБОЛОЧКИ СТАНОВЯТСЯ ВСЕ БОЛЕЕ РАСПРОСТРАНЕННЫМИ, ПОСКОЛЬКУ ВСЕ БОЛЬШЕ СЕРВЕРОВ ПОДКЛЮЧАЕТСЯ К СЕТИ

По мере того как корпоративное ИТ-пространство перемещается в сторону гибридных облачных сред, количество компаний, использующих веб-серверы, за последние несколько лет увеличилось, и во многих случаях общедоступные серверы часто имеют прямые подключения к внутренним сетям.

Как показала статистика Microsoft, злоумышленники, похоже, осознали это изменение в структуре корпоративных ИТ-сетей и усилили свои атаки на общедоступные системы.

Веб-оболочки теперь играют решающую роль в их атаках, предоставляя способ контролировать взломанный сервер и затем организовывать поворот во внутреннюю сеть цели.

Именно об этих типах атак и предупреждало Агентство национальной безопасности США в апреле 2020 года, когда оно опубликовало список из 25 уязвимостей, которые часто использовались для установки веб-оболочек.

В отчете АНБ содержится предупреждение не только о веб-оболочках, используемых в общедоступных системах, но и об их использовании во внутренних сетях, где они используются в качестве прокси-серверов для перехода к не общедоступным системам.

Microsoft призывает компании изменить приоритеты своего подхода к работе с веб-оболочками, которые постепенно становятся одной из самых серьезных угроз безопасности на сегодняшний день. В качестве способов обеспечения безопасности сети производитель ОС рекомендует несколько основных действий:

Исправляйте общедоступные системы, поскольку большинство веб-оболочек устанавливаются после того, как злоумышленники используют незащищенные уязвимости.

Распространите антивирусную защиту на веб-серверы, а не только на рабочие станции сотрудников.

Сегментация сети для ограничения повреждения зараженного сервера небольшого массива систем, а не всей сети.

Часто проверяйте и просматривайте журналы с веб-серверов, особенно для общедоступных систем, которые более уязвимы для сканирования и атак.

Соблюдайте надлежащую учетную гигиену. Ограничьте использование учетных записей с правами локального администратора или администратора домена.

Проверьте брандмауэр периметра и прокси-сервер, чтобы ограничить ненужный доступ к службам, включая доступ к службам через нестандартные порты». ***(Catalin Cimpanu. Microsoft said the number of web shells has doubled since last year // ZDNet (https://www.zdnet.com/article/microsoft-said-the-number-of-web-shells-has-doubled-since-last-year/). 12.02.2021).***

***

«Netlab, подразделение сетевой безопасности китайской охранной компании Qihoo 360, сообщило, что на этой неделе обнаружило новое вредоносное ПО, которое в настоящее время заражает устройства Android с целью создания ботнета DDoS.

Ботнет, названный Matryosh, создан для устройств Android, производители которых оставили включенным и опубликованным в Интернете интерфейс диагностики и отладки, известный как Android Debug Bridge.

Активный порт 5555, этот интерфейс был известным источником проблем для устройств Android в течение многих лет, и не только для смартфонов, но и

смарт - телевизоров, топ-набор коробок и других интеллектуальных устройств, работающих под управлением ОС Android.

За последние несколько лет семейства вредоносных программ, такие как ADB.Miner, Ares, IPStorm, Fbot и Trinity, сканировали Интернет в поисках устройств Android, где интерфейс ADB оставался активным, подключался к уязвимым системам, а также загружал и устанавливал вредоносные полезные нагрузки.

Согласно отчету, опубликованному на этой неделе, Netlab заявила, что Matryosh является последним в этой длинной череде ботнетов, нацеленных на ADB, но имеющей свою особенность.

Эта уникальность проистекает из использования сети Tor для сокрытия своих командных серверов и использования многоуровневого процесса для получения адреса этого сервера - отсюда и название ботнета, вдохновленное классическими матрешками-матрешками.

Исследователи Netlab, которые обычно одними из первых открывают новые ботнеты, говорят, что ботнет содержит несколько подсказок, позволяющих предположить, что это работа той же группы, которая разработала ботнет Moobot в 2019 году и ботнет LeetHozer в 2020 году.

Оба ботнета, по сути, были созданы и использовались для запуска DDoS-атак, что также, по-видимому, является основной функцией Матрёша.

Команда Netlab заявляет, что они обнаружили в коде функции, специфичные для функций, которые будут использовать зараженные устройства для запуска DDoS-атак через такие протоколы, как TCP, UDP и ICMP.

ОЧЕНЬ МАЛО ТОГО, ЧТО МОГУТ СДЕЛАТЬ ПОЛЬЗОВАТЕЛИ

Как было сказано в предыдущих статьях о «проблеме ADB», конечные пользователи мало что могут с этим поделать.

Хотя владельцы смартфонов могут легко отключить свою функцию ADB с помощью настройки в параметрах ОС, для других типов устройств на базе Android такая опция недоступна на большинстве устройств.

Следовательно, в результате многие системы останутся уязвимыми и подвержены злоупотреблениям на долгие годы, предоставляя ботнетам, таким как Matryosh и другие, солидную массу устройств, которые они могут использовать для крипто-майнинга, перехвата DNS или DDoS-атак». ***(Catalin Cimpanu. Android devices ensnared in DDoS botnet // ZDNet (https://www.zdnet.com/article/android-devices-ensnared-in-ddos-botnet/). 04.02.2021).***

***

«Исследователи ESET говорят, что они обнаружили легкую разновидность вредоносного ПО, которое нацелено на несколько операционных систем и поражает суперкомпьютеры, интернет-провайдеров и другие организации.

Kobalos, это неприятное программное обеспечение, как говорят, переносимо на Linux, BSD, Solaris и, возможно, AIX и Windows. Исследователи ESET Марк-Этьен М. Левей и Игнасио Санмиллан, похоже, анализировали в первую очередь

версию кода для Linux. Вот краткое изложение основных результатов их исследования:

Как он попадает на серверы, неясно, хотя системы, зараженные Kobalos, используют свой SSH-клиент для кражи имен пользователей и паролей и, предположительно, адресов серверов, которые вводятся в него. Эти данные могут быть использованы создателями вредоносного ПО для входа в эти системы и распространения своего вредоносного ПО. Это было бы особенно возможно, если бы украденные комбинации имени пользователя и пароля предназначались для учетных записей суперпользователя или sudoers. Таким образом, злоумышленники могут постепенно захватывать все больше и больше машин, по одной учетной записи за раз, всего с одного взломанного компьютера. Мы отмечаем, что для изменения SSH-клиента потребуется доступ на уровне администратора или некоторые махинации с PATH.

Kobalos обычно скрыт в исполняемом файле сервера OpenSSH зараженной машины и активирует бэкдор, если получает соединение с определенного исходного TCP-порта, обычно 55201. После установления зашифрованного соединения этот бэкдор можно использовать как удаленный терминал, выполняя произвольные команды, введенные его операторами.

Вредоносная программа также может подключаться к серверу управления и контроля (C2), который связывает программное обеспечение с его вдохновителями. Зараженный сервер также может выступать в качестве прокси между операторами и другим взломанным компьютером. Общедоступные IP-адреса и номера портов для этих машин C2 могут быть жестко запрограммированы в следующей сборке Kobalos.

По данным ESET, вредоносное ПО, а также кластеры суперкомпьютеров, были поражены крупным азиатским интернет-провайдером, североамериканским поставщиком средств защиты конечных точек, европейским маркетинговым агентством, университетскими сетями, персональными серверами людей и другим оборудованием.

ESET отдельно работала с командой компьютерной безопасности CERN, чтобы защитить сети супер-лаборатории от тех, кто собирался устанавливать майнеры криптовалюты и тому подобное на высокопроизводительных установках.

Дуэт ESET также поблагодарил Мацея Котовича из MalwareLab.pl за анализ вредоносного ПО. Приведенный выше совет содержит подробную информацию о том, как обнаружить бэкдор и как предотвратить его распространение. Рекомендуется использовать многофакторную аутентификацию для SSH, поскольку она должна предотвратить использование украденных имен пользователей и паролей. Здесь [PDF] можно найти гораздо больше технических деталей, обратного проектирования кода и использования шифрования.

ESET не желала приписывать вредоносное ПО какой-либо известной группе хакеров или национальным государствам. А что в имени? Левейе и Санмиллан сказали: «Мы назвали эту вредоносную программу Kobalos из-за ее крошечного размера кода и множества уловок; в греческой мифологии кобалос - это маленькое озорное существо».

Вредоносные программы для Linux встречаются редко, но далеко не всегда. В прошлом году Microsoft заявила о своей поддержке поиска вредоносных программ в оперативной памяти, нацеленных на серверы Linux, в то время как китайский APT41, как выяснилось, в течение пяти лет копался в различных модулях Linux». ***(Gareth Corfield. Tiny Kobalos malware seen backdooring SSH tools, menacing supercomputers, an ISP, and more – ESET // The Register (https://www.theregister.com/2021/02/03/kobalos_malware/). 03.02.2021).***

***

«Скрытая вредоносная программа TrickBot BazarBackdoor была переписана на языке программирования Nim, чтобы избежать обнаружения программным обеспечением безопасности.

Банда киберпреступников TrickBot все активнее распространяет свои новые и скрытые вредоносные программы BazarBackdoor через спам-кампании. После заражения компьютера BazarBackdoor используется для предоставления злоумышленникам удаленного доступа к компьютеру для распространения по сети.

Intezer и Advanced Intel Виталий Кремез проанализировал новый образец BazarBackdoor и обнаружил, что банда TrickBot портировала его на язык программирования Nim.

Согласно веб-сайту языка программирования, Nim черпает вдохновение из Python, Ada и Modula и может создавать исполняемые файлы, поддерживаемые в Windows, macOS и Linux.

«Nim - один из немногих программируемых языков со статической типизацией, который сочетает в себе скорость и эффективность использования памяти C, выразительный синтаксис, безопасность памяти и несколько целевых языков». говорится на веб-сайте Nim.

Поскольку вредоносное ПО, разработанное с использованием Nim, встречается редко, Кремез считает, что банда TrickBot перенесла BazarBackdoor на Nim, чтобы обойти обнаружение антивирусным программным обеспечением.

«Компонент бэкдора, способный выполнять команды, написан на языке программирования NIM, чтобы избежать обнаружения антивирусами. Преступная группа, вероятно, решила продолжить разработку облегченного вредоносного ПО в Nim, чтобы помешать антивирусу и механизму обнаружения, ориентированному на традиционные двоичные файлы, скомпилированные в Языки стиля C / C ++».

"Не так давно Golang стал еще одним предпочтительным языком для некоторых семейств вредоносных программ, включая программы-вымогатели RobbinHood, в основном из-за того, что многие антивирусные продукты не могут обрабатывать и характеризовать нетрадиционные двоичные файлы как вредоносные из-за уникального раздела и двоичного содержимого, представленного «Ним и подобные экзотические языки», - сказал BleepingComputer генеральный директор Advanced Intel Виталий Кремез.

Другое вредоносное ПО, разработанное в Nim, - это семейство программ-вымогателей под названием XCry [VirusTotal], обнаруженное командой MalwareHunterTeam в 2019 году.

Совсем недавно программа-вымогатель DeroHE с кодом Nim [VirusTotal] была использована для атаки на пользователей форума IObit.

Nim - не единственный необычный язык, который недавно использовался для создания вредоносных программ. В прошлом месяце, Kremez обнаружили, что новый Vovalex вымогатели были написаны на языке программирования D». ***(Lawrence Abrams. TrickBot's BazarBackdoor malware is now coded in Nim to evade antivirus // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/trickbots-bazarbackdoor-malware-is-now-coded-in-nim-to-evade-antivirus/). 11.02.2021).***

***

«Сегодня исследователи Unit 42 поделились информацией о новой полиморфной и «очень сложной» вредоносной программе под названием BendyBear, связанной с хакерской группой, известной связями с правительством Китая.

BendyBear также является «одним из самых сложных, хорошо спроектированных и трудно обнаруживаемых образцов шелл-кода, используемых в Advanced Persistent Threat (APT)», согласно Отчет по блоку 42 опубликован сегодня.

Хотя он был обнаружен в прошлом году, в августе 2020 года, информации о векторе заражения, использованном для его развертывания в целевых системах, или о каких-либо потенциальных жертвах нет.

Вредоносное ПО имеет функции и поведение, которые очень напоминают вредоносное ПО семейства WaterBear, которое действует по крайней мере с начала 2009 года.

WaterBear связан с BlackTech, группой кибершпионажа, связанной исследователями угроз с правительством Китая.

Эта хакерская группа из национального государства занимается кражей информации, а также подозревается в координации недавних атак, направленных на несколько правительственных организаций Восточной Азии.

Особенности и возможности вредоносного ПО

Единственная функция этого шелл-кода - использовать для загрузки других вредоносных полезных нагрузок с управляемых злоумышленником серверов управления и контроля (C2).

Кибершпионы, которые используют BendyBear в своих операциях, загружают его на взломанные устройства сразу после получения доступа к машине после эксплуатации.

«Имея более 10 000 байт, BendyBear заметно больше, чем большинство других, и использует его для реализации расширенных функций и методов антианализа, таких как модифицированное шифрование RC4, проверка блока подписи и полиморфный код», - сказал Unit 42.

Среди длинного списка функций и возможностей BendyBear, Unit 42 говорит, что это:

Передает полезные данные модифицированными фрагментами, зашифрованными RC4. Это усиливает шифрование сетевой связи, поскольку один ключ RC4 не расшифрует всю полезную нагрузку.

Попытки оставаться скрытыми от анализа кибербезопасности путем явной проверки своей среды на наличие признаков отладки.

Использует существующий раздел реестра Windows, который по умолчанию включен в Windows 10 для хранения данных конфигурации.

Очищает кеш DNS хоста каждый раз, когда он пытается подключиться к своему серверу C2, тем самым требуя, чтобы хост каждый раз разрешал текущий IP-адрес для вредоносного домена C2.

Создает уникальные сеансовые ключи для каждого подключения к серверу C2.

Скрывает свой протокол подключения, подключаясь к серверу C2 через общий порт (443), тем самым смешиваясь с обычным сетевым трафиком SSL.

Использует полиморфный код, изменяя его следы во время выполнения кода, чтобы помешать анализу памяти и избежать подписания.

Шифрует или дешифрует функциональные блоки (блоки кода) во время выполнения по мере необходимости, чтобы избежать обнаружения.

Использует позиционно-независимый код (PIC), чтобы отказаться от инструментов статического анализа.

Благодаря таким функциям, как проверка блока подписи и использование методов антианализа, довольно очевидно, что разработчики BendyBear сосредоточены на том, чтобы сделать его скрытым вредоносным ПО для уклонения от обнаружения.

Более того, его создатели демонстрируют «высокий уровень технической сложности», основанный на использовании манипуляций с байтами и пользовательских криптографических процедур.

Более подробная техническая информация о шелл-коде BendyBear, индикаторах взлома и подтверждении концепции шелл-кодом доступна в отчете Unit 42». ***(Sergiu Gatlan. New BendyBear APT malware gets linked to Chinese hacking group // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-bendybear-apt-malware-gets-linked-to-chinese-hacking-group/). 09.02.2021).***

***

«Google принудительно удалил чрезвычайно популярное расширение The Great Suspender из Google Chrome и классифицировал его как вредоносное ПО.

The Great Suspender - это расширение Chrome, которое приостанавливает неиспользуемые вкладки и выгружает их ресурсы, чтобы уменьшить использование памяти браузером. Когда пользователь готов снова использовать вкладку, ему просто нужно было щелкнуть ее, чтобы сделать ее видимой.

Это расширение пользовалось огромной популярностью у более чем 2 000 000 пользователей и неизменно рекомендовалось к использованию благодаря своей способности сокращать использование памяти Chrome.

Когда Google удалил его в четверг, пользователи остались с сообщением о том, что «Это расширение содержит вредоносное ПО», но не предоставили какой-либо дополнительной информации о том, как восстановить заблокированные вкладки или почему они его удалили.

После резкого удаления расширения The Great Suspender пользователи, у которых были приостановлены вкладки, были расстроены тем, что не могли получить к ним доступ снова.

Можно просмотреть список приостановленных вкладок с помощью встроенной функции истории Chrome и использовать этот список для восстановления URL-адреса приостановленной веб-страницы.

Инструкции о том, как это сделать, а также о других методах, можно найти на этой странице поддержки.

Падение Великой Подтяжки

В июне 2020 года разработчик The Great Suspender продал расширение неизвестной организации, так как у него не было времени должным образом поддерживать проект.

В то время пользователи с подозрением относились к продаже: зачем компании покупать бесплатное расширение с открытым исходным кодом, которое не приносит разработчикам дохода.

Поскольку бесплатные расширения покупались в прошлом, а затем монетизировались с помощью вредоносных изменений, таких как внедрение рекламы или кража информации, пользователи были обеспокоены тем, что то же самое может случиться с The Great Suspender.

К сожалению, опасения пользователя были оправданы, когда новый сопровождающий обновил расширение в октябре 2020 года до версии 7.1.8, которая включала скрипты, отслеживающие поведение пользователя и выполнявшие код, полученный с удаленного сервера.

Эта вредоносная деятельность привела к тому, что Microsoft удалила расширение Microsoft Edge Store и выпустила новую версию 7.1.9 без вредоносных скриптов.

Однако расширение продолжало оставаться в руках этих неизвестных разработчиков, которые могли внедрить вредоносный код позже, возможно, незаметно для пользователей.

В четверг Google объявил расширение Chrome Web Store вредоносным, но не представил никаких причин для этого. Неясно, обнаружил ли Google дополнительные вредоносные скрипты или отреагировал на их историю и опасения сообщества.

Для тех, кто действительно хочет использовать расширение The Great Suspender, на странице проекта GitHub по-прежнему предлагается версия 7.1.6, которая является окончательной версией расширения, принадлежащей исходному разработчику, и не содержит вредоносных скриптов.

Чтобы установить расширение, вам нужно будет сделать это в режиме разработчика Chrome, что не рекомендуется, так как оно устраняет преимущества безопасности, предлагаемые процессом проверки расширений Google». ***(Lawrence Abrams. The Great Suspender Chrome extension's fall from grace // Bleeping***

Computer® (https://www.bleepingcomputer.com/news/software/the-great-suspender-chrome-extensions-fall-from-grace/). 06.02.2021).

***

«LodaRAT, известный своей нацеленностью на устройства Windows, также был обнаружен нацелившимся на устройства Android в рамках новой шпионской кампании.

Недавно обнаруженный вариант вредоносной программы LodaRAT, которая исторически нацелена на устройства Windows, распространяется в рамках продолжающейся кампании, которая теперь также выслеживает устройства Android и шпионит за жертвами.

Наряду с этим также была обнаружена обновленная версия LodaRAT для Windows; Обе версии были замечены в недавней кампании, нацеленной на Бангладеш, говорят исследователи.

Кампания отражает всеобъемлющий сдвиг в стратегии разработчиков LodaRAT, поскольку атака, по всей видимости, вызвана шпионажем, а не ее предыдущими финансовыми целями. В то время как предыдущие версии LodaRAT содержали возможности кражи учетных данных, которые, по предположениям исследователей, использовались для опустошения банковских счетов жертв, эти новые версии поставляются с полным набором команд для сбора информации.

«Тот факт, что группа угроз превратилась в гибридные кампании, нацеленные на Windows и Android, показывает, что группа процветает и развивается», - заявили исследователи из Cisco Talos во вторник. «Наряду с этими улучшениями, злоумышленник теперь сосредоточился на конкретных целях, что указывает на более зрелые операционные возможности. Как и в случае с более ранними версиями Loda, обе версии этой новой итерации представляют серьезную угрозу, поскольку могут привести к серьезной утечке данных или серьезным финансовым потерям».

Что такое вредоносное ПО LodaRAT?

LodaRAT, впервые обнаруженный в сентябре 2016 года, представляет собой троян удаленного доступа (RAT), который обладает множеством возможностей для слежки за жертвами, такими как запись микрофонов и веб-камер устройств жертв. Название «Loda» происходит от каталога, в который автор вредоносного ПО решил вести журналы кейлоггеров.

С момента своего открытия в 2016 году RAT быстро распространился, и в сентябре в дикой природе было обнаружено несколько новых версий. RAT, который написан на AutoIT, по-видимому, распространяется несколькими группами киберпреступников, которые использовали его для нацеливания на многочисленные вертикали.

Недавняя кибератака LodaRAT в Бангладеш

Исследователи наблюдали за кампанией с участием LodaRAT, которая началась в октябре и продолжается до сих пор. Злоумышленники проявляют особый интерес к организациям в Бангладеш, включая банки и поставщиков программного обеспечения для передачи голоса по IP (VoIP) операторского уровня.

Витор Вентура, технический руководитель Cisco Talos и старший исследователь безопасности, сообщил Threatpost, что первоначальные векторы атаки для кампании включали электронные письма, отправленные жертвам со ссылками на вредоносные приложения (включая версии для Windows и Android) или вредоносные документы (включая только Windows версия).

«Кампания выявила таргетинг на Бангладеш с использованием различных уровней приманок, от доменов, сквотированных типами, до имен файлов, напрямую связанных с продуктами или услугами их жертв», - заявили исследователи.

Для атаки maldoc, нацеленной на Windows, после того, как жертва щелкнула вредоносные документы, злоумышленники использовали вредоносный RTF-документ, который использует CVE-2017-11882 (уязвимость удаленного выполнения кода, существующую в Microsoft Office), чтобы затем загрузить LodaRAT.

Новый вариант Android от LodaRAT

По словам исследователей, версия вредоносного ПО LodaRAT для Android, которую исследователи называют «Loda4Android», «относительно проста по сравнению с другими вредоносными программами для Android». Например, RAT специально избегает техник, часто используемых банковскими троянами Android, таких как использование API доступности для кражи данных.

По словам исследователей, лежащий в основе протокол управления и контроля (C2) следует тому же шаблону проектирования, что и версия для Windows, предполагая, что код C2 сможет обрабатывать обе версии.

Кроме того, по словам исследователей, Loda4Android имеет «все компоненты приложения-сталкера». Вредоносная программа собирает данные о местоположении и записывает аудио, а также может делать фотографии и снимки экрана.

«Он может записывать аудиозвонки, но будет записывать только то, что говорит жертва, но не то, что говорит собеседник», - заявили исследователи. «Также присутствуют общие функции SMS, журнала вызовов и утечки контактов. Интересно отметить, что он не способен перехватывать SMS или звонки, как это обычно бывает в банковских троянах».

Свежая версия Windows Loda

Новая версия LodaRAT, предназначенная для систем Windows, - это версия 1.1.8. Хотя он в основном такой же, как и предыдущие версии, были добавлены новые команды, расширяющие его возможности.

Во-первых, версия поставляется с новыми командами, которые предоставляют злоумышленнику удаленный доступ к целевой машине через протокол удаленного рабочего стола (RDP). В новой версии теперь можно использовать аудиотеку BASS для захвата звука с подключенного микрофона. BASS используется в программном обеспечении Win32, macOS, Linux и PocketPC для обеспечения функций потоковой передачи и записи музыки.

«Эта новая команда является улучшением предыдущей команды« Звук», которая использовала встроенный в Windows Sound Recorder», - заявили исследователи. «Причина отказа от предыдущего метода, вероятно, связана с тем,

что Windows Sound Recorder может записывать звук только в течение максимум 60 секунд. Новый метод позволяет вести запись в любое время, указанное злоумышленником». ***(Lindsey O'Donnell. Android Devices Hunted by LodaRAT Windows Malware // Threatpost (https://threatpost.com/android-devices-lodarat-windows/163769/). 09.02.2021).***

***

«Инструменты Enhanced Explosive RAT и Caterpillar находятся в авангарде глобальной шпионской кампании.

По словам исследователей, с начала 2020 года группа продвинутых постоянных угроз (APT) Lebanese Cedar скомпрометировала не менее 250 общедоступных серверов с помощью своего последнего вредоносного ПО.

Группа добавила новые функции в свою пользовательскую веб-оболочку «Caterpillar» и троян удаленного доступа (RAT) «Explosive RAT», оба из которых исследователи ClearSky Security заявили, что они связаны с компрометацией общедоступных серверов [PDF], что позволило широко распространить шпионаж.

«Целевые компании находятся во многих странах, в том числе: в США, Великобритании, Египте, Иордании, Ливане, Израиле и Палестинской автономии», - говорят исследователи. «По нашим оценкам, есть еще много компаний, которые были взломаны, и что ценная информация была украдена у этих компаний в течение нескольких месяцев и лет».

Обновление для Explosive RAT

Визитная карточка Ливанского кедра - поиск уязвимых систем. По словам ClearSky, последняя, четвертая версия Explosive RAT использовалась против неустановленных веб-серверов Oracle (CVE-2012-3152) и Atlassian (CVE-2019-3396 и CVE-2019-11581). Эта группа также является единственной группой APT, которая, как известно, использует код Explosive RAT, добавил ClearSky.

ClearSky заявила, что определила конкретные обновления, внесенные в новую Explosive RAT по сравнению с предыдущей версией, которая впервые была использована еще в 2015 году, а именно анти-отладку и зашифрованную связь между скомпрометированной машиной и сервером управления и контроля (C2).

«Explosive использует несколько методов уклонения, чтобы избежать обнаружения и поддерживать постоянство, такие как обфускация, шифрование связи и использование отдельной DLL для работы API», - говорится в отчете ClearSky. «С 2015 года в инструмент были внесены незначительные изменения в области обфускации и шифрования связи. Сеть управления RAT хорошо продумана. Он состоит из жестко заданных по умолчанию серверов C2, статических серверов обновлений и динамических серверов обновлений на основе DGA».

Согласно ClearSky, у нового Explosive RAT есть дополнительное новое шпионское оружие, которое можно использовать и против систем, такое как кейлоггинг, захват снимков экрана и выполнение команд, что делает угрозу как устойчивой, так и незаконной.

«Возможности вредоносного ПО по сбору данных являются как пассивными, так и активными - оно собирает данные, обнаруженные на взломанной машине, и

имеет возможность поиска данных по запросу», - сообщает ClearSky. «Explosive также имеет такие функции, как идентификация машин, мониторинг использования памяти для обеспечения скрытности, удаленная оболочка и выполнение произвольного кода».

Обновления веб-оболочки

Последний набор вредоносных программ Ливанского кедра также использует вторую версию веб-оболочки Caterpillar для широкого сбора сетевых данных и установки файлов в целевые системы.

«Выступая в качестве координационного центра, группа обычно атакует веб-серверы через специальную веб-оболочку, а именно Caterpillar - вариант веб-оболочки с открытым исходным кодом ASPXspy», - говорится в отчете ClearSky. «Используя веб-оболочку, злоумышленники оставляют свои отпечатки пальцев на веб-сервере и внутренней сети, перемещаются по сторонам и развертывают дополнительные инструменты».

В отчете добавлено, что Caterpillar намеревается найти потенциально ценные данные, установить файлы конфигурации сервера и даже получить доступ к паролям и именам пользователей.

Группа использует веб-оболочку для передачи данных на сервер C2 через службы VPN NordVPN или ExpressVPN, поясняется в отчете, а затем устанавливает файловый браузер.

По наблюдениям ClearSky, ливанский кедр использует свою сигнатуру Explosive RAT, а не веб-оболочки.

«Сама ТТП [тактика, техника и процедура] была изменена», - объясняет ClearSky. «В 2015 году Lebanese Cedar в основном полагалась на Explosive RAT в качестве основного инструмента. В недавней кампании мы выявили несколько веб-панелей Caterpillar и меньшее использование Explosive RAT (на основе наших сканирований). Соответственно, мы предлагаем, что основным вектором развития ливанского кедра в 2020 году будет использование веб-оболочки».

Государственный актер, Ливанский кедр

Ливанский кедр, также известный как «Летучий кедр», появился в 2012 году и связан с кибер-подразделением «Хезболлы», согласно Check Point, который добавил, что группа выбирает цели на основе политики и идеологии. Хезболла - это политическая партия и боевая группировка, базирующаяся в Ливане.

В 2015 году исследователи Check Point также связали группу APT с правительством Ливана.

«Ливанский кедр, известный своими очень ускользающими, избирательно направленными и тщательно управляемыми операциями, следует курсам действий, связанным с APT, финансируемыми национальными государствами или политическими группами», - добавлено в отчете.

В прошлом жертвы в основном работали в телекоммуникационном и ИТ-секторах по всему миру, включая Египет, Израиль, Иорданию, Палестинскую администрацию, Великобританию и США.

«Арсенал Lebanese Cedar APT состоит из полноценной веб-оболочки, специально разработанной RAT и набора тщательно отобранных дополнительных инструментов, включая инструменты грубой силы URI», - сообщает CheckPoint.

«Группа использует инструменты с открытым исходным кодом наряду со своими собственными инструментами, включая пользовательскую веб-оболочку, скорее всего, созданную иранскими группами хактивистов, такими как «ITSecTeam» и «Persian Hacker».

Иван Риги, аналитик разведки угроз из Digital Shadows, сказал Threatpost, что, по его мнению, APT «вероятно, проводил эту кампанию, чтобы поддержать мотивы Хезболлы получить конфиденциальную информацию».

Патчем, народ!

Поскольку группа использует эксплойты для уязвимостей, чтобы получить первоначальный доступ к целям, исправление - лучшая первая защита от подобных атак.

«Тот факт, что 250 систем были скомпрометированы, уже свидетельствует о важности исправления этих решений, особенно при использовании в контексте сотрудничества между сторонами, предприятиями и государственными учреждениями», - пояснил Threatpost Дирк Шрейдер, глобальный вице-президент New Net Technologies. «Как всегда, лучшая защита - это обеспечение хорошей кибергигиены, сканирование на наличие уязвимостей, исправление, где это возможно, и контроль любых изменений, происходящих в инфраструктуре между сканированиями».

Тал Моргенштерн из Vulcan Cyber согласился с тем, что соблюдение элементарных правил безопасности по-прежнему является лучшей линией защиты для организаций. Он объяснил, что злоумышленники рыщут в поисках дыр, которые, как им известно, уже существуют.

«Злоумышленники продолжают использовать известные уязвимости в своих целях. В этом случае уязвимые общедоступные веб-сайты используются для распространения вредоносного ПО, в результате чего ничего не подозревающие посетители становятся жертвами чего-то, что можно исправить с помощью патча или изменения конфигурации».

Призыв к сотрудничеству в сфере информационной безопасности

В целом, лучший вариант против Ливанского кедра и других подобных угроз - более тесное сотрудничество между поставщиками, исследователями, отраслевыми группами и правоохранительными органами, сообщил Threatpost Дерек Мэнки из FortiGuard Labs компании Fortinet.

«Например, многие организации, занимающиеся безопасностью, предоставляют пособия по защите от состязательных угроз, которые могут предоставить актуальный анализ и информацию о последних группах APT и вредоносных кампаниях на сегодняшний день, с целью предоставления службам быстрого реагирования, защитников сети и всем, кто интересуется, полезной информацией - сказал Мэнки по электронной почте. «Кроме того, организациям необходимо будет знать, кого информировать в случае атаки, чтобы «отпечатки пальцев» могли быть надлежащим образом переданы и правоохранительные органы могли выполнять свою работу».

Помимо базового междисциплинарного сотрудничества, Мэнки сказал, что для сообщества безопасности будет все более важно начать работать вместе как единый глобальный фронт.

«Киберпреступники не имеют границ в сети, поэтому борьба с киберпреступностью также должна выходить за рамки границ», - добавил Мэнки. «Только совместными усилиями мы сможем переломить ситуацию с киберпреступниками». ***(Becky Bracken. Hezbollah-Linked Lebanese Cedar APT Infiltrates Hundreds of Servers // Threatpost (https://threatpost.com/hezbollah-lebanese-cedar-apt-servers/163555/). 01.02.2021).***

***

«Компания Palo Alto Networks сообщает, что хакерская группировка Rocke использует новую майнинговую малварь Pro-Ocean для атак на уязвимые установки Apache ActiveMQ, Oracle WebLogic и Redis.

Напомню, что Rocke была обнаружена экспертами Cisco Talos еще далеким летом 2018 года. Основным направлением работы группы всегда был майнинг криптовалюты Monero, и мы рассказывали о том, как хакеры конкурировали с другими злоумышленниками за контроль над уязвимыми серверами.

Теперь эксперты пишут, что Rocke по-прежнему не изменяет своей привычке атаковать облачные приложения и эксплуатировать различные известные уязвимости для захвата контроля над непропатченными серверами Oracle WebLogic (CVE-2017-10271), Apache ActiveMQ (CVE-2016-3088) и небезопасными установками Redis.

Обнаруженная аналитиками малварь Pro-Ocean содержит «новые и улучшенные» возможности, лежащие в области руткитов и червей. Эти функции позволяют Pro-Ocean эффективно скрывать свою вредоносную активность.

К примеру, чтобы оставаться незамеченной, Pro-Ocean использует функцию Linux LD_PRELOAD, которая помогает приоритизировать загрузку определенных библиотек, а также библиотеку Libprocesshider.

Как было замечено выше, Pro-Ocean обладает потенциалом червя, и реализовано такое распространение малвари весьма просто. Специальный Python-скрипт использует общедоступный IP-адрес зараженной машины и службу identity.me, а затем пытается заразить любые доступные машины, находящиеся в той же 16-битной подсети. При этом малварь не старается как-то отсортировать потенциальных жертв и просто пытается применить эксплоиты к любым обнаруженным хостам в надежде, что один из них сработает. В случае успеха скрипт доставляет в систему полезную нагрузку, которая, в свою очередь, загружает скрипт для установки для Pro-Ocean с удаленного HTTP-сервера.

Этот написанный на Bash и обфусцированный установочный скрипт играет важную роль в операциях Rocke. Дело в том, что помимо доставки на зараженный хост малвари Pro-Ocean, он же устраняет конкурентов, удаляя любые вредоносы и майнеры, уже присутствующие в системе. Кроме того, скрипт предоставляет Pro-Ocean полный доступ, удаляя iptables Firewall и любые агенты мониторинга, которые могут заметить атаку и понять тревогу.

Так как майнинг Monero – по-прежнему приоритетная задача хакеров, Pro-Ocean поставляется со специальным модулем, который следит за использованием ЦП и ликвидирует любые легитимные процессы, если те загружают процессор

более чем на 30%. Этот же модуль регулярно проверяет, активен ли майнер и перезапускает его, если что-то пошло не так.

Исследователи предупреждают, что пока малварь использует лишь две уязвимости, но в будущем их количество может увеличиться, если авторы малвари решат нацелить Pro-Ocean на другие облачные приложения и серверы. Пока же специалисты уверены, что главными целями для атак Pro-Ocean являются облачные сервисы Alibaba и Tencent». ***(Мария Нефёдова. Майнинговый вредонос Pro-Ocean атакует серверы Apache, Oracle и Redis // Xakep (https://xakep.ru/2021/02/02/pro-ocean/). 02.02.2021).***

***

«Исследователи компании Check Point рассказали о новом вредоносном ПО для Office, распространяющемся через фишинговые электронные письма. Операторы вредоноса атаковали более 80 клиентов Check Point по всему миру с целью захвата контроля над компьютерами и удаленного похищения информации.

Используемый злоумышленниками инструмент APOMacroSploit представляет собой генератор макро-эксплоитов, позволяющий создавать документы Excel, способные обходить решения безопасности, Windows Antimalware Scan Interface (AMSI), механизмы безопасности Gmail и другие средства для защиты от фишинга. Вредонос является делом рук французских киберпреступных группировок Apocaliptique и Nitrix. По подсчетам исследователей, на продажах APOMacroSploit на киберпреступном форуме HackForums.net за один месяц они заработали $5 тыс.

За вредоносной кампанией стоят сорок киберпреступников, которые используют сто разных отправителей электронных писем для атак на жертв в более тридцати странах мира. Впервые атаки были обнаружены в конце ноября 2020 года.

Заражение вредоносным ПО начинается, когда включается динамическое содержимое прикрепленного к фишинговом письму XLS-документа, и макрос XLM автоматически начинает загрузку командного скрипта для Windows. Скрипт извлекается из файла cutt.ly, направляющего на серверы, где размещено несколько BAT-скриптов, к именам файлов которых привязаны никнеймы пользователей. Скрипты также отвечают за выполнение вредоносного ПО («fola.exe») на системах под управлением Windows, но не раньше добавления местоположения вредоносного ПО в путь исключений Защитника Windows и отключения очистки Windows». ***(Эксперты установили, кто стоит за конструктором вредоносного ПО APOMacroSploit // SecurityLab.ru (https://www.securitylab.ru/news/516740.php). 18.02.2021).***

***

«Фахівці з кібербезпеки з Check Point Research опублікували результати свіжого дослідження. На основі отриманих даних вони назвали найнебезпечніший комп'ютерний вірус початку 2021 року.

Так, вже другий місяць поспіль лідером серед шкідливого ПЗ залишається Emotet, розповіли представники компанії. За їх словами, жертвою ботнету залишаються близько 6% організацій по всьому світу.

При цьому своєчасна реакція правоохоронних органів призвела до помітного зниження активності Emotet, а саме на 14%. За словами поліцейських, вони мають намір видалити вірус з заражених хостів вже 25 квітня 2021 року.

Нагадаємо, що вперше про найнебезпечніший на сьогоднішній день вірус стало відомо в 2014 році. За останні 7 років троян активно розвивався і оновлювався, в результаті чого залишався актуальним і високоефективним.» ***(Кіберфахівці визначили найнебезпечніший комп'ютерний вірус початку року // BusinessUA.Com (http://businessua.com/telekom/67919kiberfahivci-viznachili-nainebezpechnishii-kompyuternii-virus-pochatku-roku.html#). 21.02.2021).***

***

«Популярное приложение для Android Barcode Scanner, с помощью которого можно сканировать шрих-коды превратилось во вредоносное ПО и заразило миллионы смартфонов пользователей. Согласно данным компании Malwarebytes, данное приложение установили более десяти миллионов раз, сообщает "Лента.ру".

Barcode Scanner является доступным в официальном магазине Google Play, которым пользуются владельцы устройств на операционной системе Android. Сообщается, что первое время программа не имела никаких вредоносных характеристик, соответственно не вызывая подозрений со стороны пользователей. Однако в последнем обновлении эксперты обнаружили опасную функцию, о которой ничего не указывалось в описании приложения. В компанию Malwarebytes, специализирующуюся на вопросах кибербезопасности, начали поступать сообщения с жалобами от пользователей Они утверждали, что теперь в браузере стали сами по себе открываться страницы с рекламой. Эксперты, изучившие программный код Barcode Scanner, пришли к выводу, что именно от него исходит атака объявлениями с целью получения заработка от их показа. Специалист Malwarebytes Нэйтан Коллиер сообщил о наличии опасного приложения компании Google, после чего Barcode Scanner удалили из магазина. Однако программа все еще работает у всех, кто не удалил ее самостоятельно со своих смартфонов…» ***(Елизавета Черных. Популярное приложение заразило миллионы смартфонов вредоносным содержимым // Comments.ua (https://it.comments.ua/news/technology/populyarnoe-prilozhenie-zarazilo-milliony-smartfonov-vredonosnym-soderzhimym-671494.html). 10.02.2021).***

***

«Почти 30 тысяч устройств Mac от Apple по всему миру заражены зловредным ПО непонятного назначения. Специалисты по кибербезопасности обеспокоены, ведь данная сетевая угроза имеет сложную природу. Как сообщает IXBT, угрозу нашла команда исследователей Red Canary. Новую разновидность вредоносного ПО назвали Silver Sparrow.

Отмечается, что вредоносная программа является странной по ряду причин. Прежде всего, потому, что до сих пор оставалась в основном бездействующей. Несмотря на то, что она обменивается данными с управляющими серверами один

раз в час, на данный момент Silver Sparrow не нанёс вреда заражённым компьютерам.

У Silver Sparrow есть варианты как для старых процессоров Intel x86_64, так и для нового Apple M1. Обе версии содержат «двоичные файлы сторонних наблюдателей», которые при запуске выводят сообщения «Hello World!» и «Ты сделал это!».

Отмечается, что вывод подобных сообщений на экран не является серьёзной проблемой, но потенциально зловред может начать выполнять определенные функции по запросу с серверов управления.

В Red Canary подчеркнули, что сложная инфраструктура эффективно использует сети CDN и AWS, что затрудняет отслеживание и удаление.

Кроме того, Silver Sparrow содержит механизмы самоуничтожения, которые удаляют все следы вредоносного ПО с заражённых устройств. Этот механизм не наблюдался по умолчанию на заражённых компьютерах, а это означает, что он был загружен произвольно на основе выполнения неизвестных в настоящее время условий.

По данным исследователей, по состоянию на 17 февраля 2021 было заражено 29 139 устройств с macOS, которые находятся в 153 странах». ***(Почти 30 тысяч устройств под macOS по всему миру заразились таинственным вирусом // RUpor.info (https://www.rupor.info/news/170102/pochti-30-tysyach-ustroystv-pod-macos-po-vsemu-miru-zarazilis-tainstvennym-virusom). 23.02.2021).***

***

«Количество штаммов вредоносных программ, закодированных на языке программирования Go, резко увеличилось примерно на 2000% за последние несколько лет, с 2017 года, говорится в отчете компании Intezer, занимающейся кибербезопасностью, на этой неделе.

Выводы компании подчеркивают и подтверждают общую тенденцию в экосистеме вредоносных программ, где авторы вредоносных программ постепенно отошли от C и C ++ к Go, языку программирования, разработанному и запущенному Google в 2007 году.

INTEZER: ВРЕДОНОСНЫЕ ПРОГРАММЫ ТЕПЕРЬ СТАЛИ ОБЫЧНЫМ ЯВЛЕНИЕМ

Хотя первое вредоносное ПО на основе Go было обнаружено в 2012 году, Golang потребовалось несколько лет, чтобы завоевать популярность среди вредоносных программ.

«До 2019 года обнаружение вредоносных программ, написанных на Go, было более редким явлением, а в течение 2019 года это стало повседневным явлением», - говорится в отчете Intezer.

Но сегодня Golang (как его часто также называют вместо Go) прорвался и получил широкое распространение.

Он используется хакерскими группами на национальном уровне (также известными как APT), операторами киберпреступности и даже группами безопасности, которые часто использовали его для создания наборов инструментов для тестирования на проникновение.

Есть три основные причины, по которым Голанг стал свидетелем внезапного резкого роста популярности. Во-первых, Go поддерживает простой процесс кроссплатформенной компиляции. Это позволяет разработчикам вредоносных программ один раз писать код и компилировать двоичные файлы из одной и той же кодовой базы для нескольких платформ, позволяя им ориентироваться на Windows, Mac и Linux из одной и той же кодовой базы - универсальности, которой они обычно не обладают со многими другими языками программирования.

Вторая причина заключается в том, что двоичные файлы на основе Go по-прежнему сложно анализировать и подвергать обратному проектированию исследователям безопасности, что позволяет поддерживать очень низкие уровни обнаружения вредоносных программ на основе Go.

Третья причина связана с поддержкой Go для работы с сетевыми пакетами и запросами. Intezer объясняет:

«Go имеет очень хорошо написанный сетевой стек, с которым легко работать. Go стал одним из языков программирования для облака, на котором написано множество нативных облачных приложений. Например, Docker, Kubernetes, InfluxDB, Traefik, Terraform, CockroachDB, Prometheus и Consul - все написаны на Go. Это имеет смысл, учитывая, что одной из причин создания Go было изобретение лучшего языка, который можно было бы использовать для замены внутренних сетевых сервисов C ++, используемых Google».

Поскольку штаммы вредоносных программ обычно подделывают, собирают или отправляют / получают сетевые пакеты все время, Go предоставляет разработчикам вредоносных программ все необходимые инструменты в одном месте, и легко понять, почему многие разработчики вредоносных программ отказываются ради этого от C и C ++. По этим трем причинам мы увидели больше вредоносных программ Golang в 2020 году, чем когда-либо прежде.

«Многие из этих вредоносных программ [семейств] представляют собой бот-сети, нацеленные на устройства Linux и IoT, чтобы либо установить крипто-майнеры, либо зарегистрировать зараженную машину в бот-сетях DDoS. Кроме того, программы-вымогатели были написаны на Go и, похоже, становятся все более распространенными», - сказал Интезер.

Примеры некоторых из самых больших и наиболее распространенных угроз на основе Go, замеченных в 2020 году, включают в себя (по категориям):

Национальное вредоносное ПО APT:

Zebrocy - российская группа APT28, спонсируемая государством, в прошлом году создала версию своего вредоносного ПО Zebrocy на базе Go.

WellMess - Российская государственная группа APT29 в прошлом году развернула новые обновленные версии своего вредоносного ПО WellMess на базе Go.

Godlike12 - Группа, спонсируемая китайским государством, в прошлом году использовала бэкдоры на основе Go для атак на тибетское сообщество.

Go Loader - Связанный с Китаем Mustang Panda APT в прошлом году развернул новый загрузчик на базе Go для своих атак.

Вредоносное ПО для электронных преступлений:

GOSH - Печально известная группа Carbanak развернула новую RAT по имени GOSH, написанную на Go в августе прошлого года.

Glupteba - В 2020 году были представлены новые версии загрузчика Glupteba, более совершенные, чем когда-либо.

Новый RAT ориентации серверов Linux под управлением Oracle WebLogic был замечен Bitdefender.

CryptoStealer.Go - Новые и улучшенные версии вредоносного ПО CryptoStealer.Go были замечены в 2020 году. Это вредоносное ПО предназначено для кошельков с криптовалютой и паролей браузеров.

Кроме того, в течение 2020 года был обнаружен похититель буфера обмена, написанный на Go.

Новые штаммы вымогателей, написанные на Go:

РоббинГуд

Нефилим

ЭКАНС

Естественно, в свете своих недавних открытий Intezer, наряду с другими, ожидает, что использование Golang продолжит расти в ближайшие годы и присоединится к C, C ++ и Python в качестве предпочтительного языка программирования для кодирования вредоносных программ в будущем». ***(Catalin Cimpanu. Go malware is now common, having been adopted by both APTs and e-crime groups // ZDNet (https://www.zdnet.com/article/go-malware-is-now-common-having-been-adopted-by-both-apts-and-e-crime-groups/). 26.02.2021).***

***

Програми-вимагачі

«Два члена теневого министерства труда призвали к национальной стратегии вымогателей, один из которых, по их словам, направлен на сокращение количества таких атак на австралийские цели.

В отчете [PDF], подготовленном теневым министром внутренних дел Кристиной Кенили и теневым помощником министра связи Тимом Уоттсом, лейбористы заявили, что из-за того, что программы-вымогатели являются самой большой угрозой для Австралии, пришло время разработать стратегию по предотвращению этого.

«Австралии нужна комплексная национальная стратегия в отношении программ-вымогателей, призванная снизить привлекательность австралийских целей в глазах киберпреступников», - говорится в отчете.

«Ни одно из этих вмешательств не является серебряной пулей. Но угроза программ-вымогателей никуда не денется, и правительство не может предоставить австралийским организациям решать эту проблему в одиночку».

В отчете указывается на неутешительную стратегию кибербезопасности правительства Австралии, опубликованную в августе.

«[В нем] правильно указано, что отдельные организации несут основную ответственность за защиту своих сетей от любых киберугроз, включая программы-вымогатели. Однако это далеко не конец истории», - говорится в отчете.

В нем также говорится, что у правительства есть ряд инструментов политики, которые только оно может использовать для сокращения общего объема атак с использованием программ-вымогателей, таких как принятие нормативных актов, правоохранительные органы, дипломатия, заключение международных соглашений, наступательные кибероперации, а также введение санкций.

«В то время как отдельные организации всегда будут нести основную ответственность за безопасность своих сетей, правительства могут стратегически вмешаться, чтобы сформировать общую среду угроз таким образом, чтобы сделать австралийские цели менее привлекательными», - продолжил он.

Одно из предложений, сделанных в отчете, состоит в том, чтобы правительство Австралии следовало подходу, направленному на изменение окупаемости инвестиций групп программ-вымогателей, нацеленных на австралийские организации.

«Для этого он должен реализовывать ряд инициатив, направленных на увеличение затрат на проведение кампаний против австралийских организаций и снижение прибыли, получаемой от таких кампаний», - говорится в сообщении.

«У австралийского правительства есть инструменты, которые оно может использовать, чтобы возложить расходы на бригады вымогателей, нацеленных на австралийцев, включая действия правоохранительных органов, целевые международные санкции и наступательные кибероперации».

Кроме того, в отчете говорится, что, хотя австралийские правоохранительные органы участвовали в некоторых важных историях успеха международного сотрудничества в области киберпреступности, австралийские правоохранительные органы должны более активно и заметно участвовать в международных операциях против операторов программ-вымогателей и преследовании тех, кто нацелен на Австралию.

В нем говорится, что в случае, если нет никаких перспектив для правоохранительных действий против групп вымогателей, Австралии следует попытаться возложить расходы на команды вымогателей, которые нацелены на австралийские организации, пытаясь помешать их деятельности с помощью наступательных кибероперациий.

Лейбористская партия также считает, что Австралия могла бы сделать больше для разработки программ предотвращения киберпреступлений, таких как использование существующих программ помощи для разработки программ диверсии и разработка квалифицированных путей миграции для «молодых, технически подкованных людей» в Индо-Тихоокеанском регионе.

Другой способ, которым теневые министры считают, что правительство может стремиться уменьшить отдачу от атак программ-вымогателей на австралийские организации, - это нацеливаться на обмены криптовалютой, которые позволяют осуществлять платежи программ-вымогателей.

«Криптовалюты были решающей технологией, способствующей росту числа программ-вымогателей, поскольку они обеспечивали анонимную систему выплаты

выкупа за пределами существующей глобальной платежной архитектуры», - пишут они. «Отсутствие центральной организации, контролирующей криптовалюты, сделало соблюдение существующих законов о борьбе с отмыванием денег «знай своего клиента» намного более сложной задачей в этом контексте».

В заключении отчета говорится, что, возможно, самый простой способ снизить отдачу от атак программ-вымогателей на австралийские организации - это повысить общий уровень устойчивости ИТ-сетей австралийских организаций.

В другом месте глава отдела информационной войны министерства обороны Австралии генерал-майор Сьюзан Койл использовала свое выступление на конференции IBM Think Australia и Новой Зеландии в четверг, чтобы сказать, что важно исправлять системы и часто менять пароли.

«Прежде всего, мы должны признать, что существует риск, и мысль об отсутствии риска делает нас более самоуверенными», - сказала она». ***(Asha Barbaschow. Labor calls for an Australian ransomware strategy // ZDNet (https://www.zdnet.com/article/labor-calls-for-an-australian-ransomware-strategy/). 18.02.2021).***

***

«Польский разработчик игр CD Projekt Red, производитель игр категории Triple A, таких как Cyberpunk 2077 и The Witcher, раскрыл сегодня атаку с использованием программ-вымогателей.

В сообщениях, размещенных на ее официальных каналах в социальных сетях, игровая студия сообщила, что атака произошла вчера, когда злоумышленник получил доступ к корпоративной сети компании.

«Хотя некоторые устройства в нашей сети были зашифрованы, наши резервные копии остаются нетронутыми. Мы уже защитили нашу ИТ-инфраструктуру и начали восстановление данных», - написала компания в Facebook и Twitter.

Производитель игры также опубликовал копию записки о выкупе, в которой хакеры утверждали, что получили копии исходного кода таких игр, как Cyberpunk 2077, Gwent и The Witcher 3, а также неизданную версию игры The Witcher 3.

Но, несмотря на угрозу утечки информации, производитель игр заявил, что не будет платить выкуп.

«Мы не будем уступать требованиям и не будем вести переговоры с действующим лицом, зная, что это может в конечном итоге привести к раскрытию скомпрометированных данных», - заявили в компании.

«Мы все еще расследуем инцидент, однако в настоящее время можем подтвердить, что - насколько нам известно - скомпрометированные системы не содержали никаких личных данных наших игроков или пользователей наших сервисов».

Производитель игры заявил, что уже уведомил местные власти. Это также второй раз, когда польская компания подверглась нападению банды вымогателей. Он стал жертвой аналогичного инцидента в июне 2017 года.

CD Projekt Red теперь становится четвертой крупной игровой студией, ставшей жертвой атаки вымогателей за последние 12 месяцев после атак на Ubisoft

и Crytek со стороны банды Egregor и атаки на Capcom со стороны банды Ragnar Locker.

По словам исследователя безопасности Emsisoft, злоумышленник, стоящий за атакой CD Projekt Red, был идентифицирован как банда вымогателей под названием HelloKitty». ***(Catalin Cimpanu. CD Projekt Red game studio discloses ransomware attack, extortion attempt // ZDNet (https://www.zdnet.com/article/cd-projekt-red-game-studio-discloses-ransomware-attack-extortion-attempt/). 09.02.2021).***

***

«UL LLC, более известная как Underwriters Laboratories, подверглась атаке программ-вымогателей, которые зашифровали ее серверы и вынудили их выключить системы на время восстановления.

UL - крупнейшая и старейшая компания по сертификации безопасности в Соединенных Штатах, с 14 000 сотрудников и офисами в более чем 40 странах.

Если вы когда-либо смотрели на заднюю часть электроприбора, ноутбука, пульта дистанционного управления от телевизора, лампочки или даже на зарядное устройство Apple USB, логотип UL, отпечатанный на устройстве, становится легко узнаваемым.

Когда компании выпускают новые продукты, они обычно представляют их в UL для тестирования и сертификации в соответствии с национально признанными стандартами безопасности и устойчивого развития. В зависимости от того, какие тесты были проведены и их результаты, продукт получит различные сертификаты UL.

Помимо сертификатов безопасности продуктов, UL также разрабатывает очень популярные 3DMark, PCMark и VRMark утилит для тестирования ПК и графики.

В минувшие выходные UL была атакована программой-вымогателем.

…на прошлых выходных UL подверглась атаке программы-вымогателя, которая зашифровала устройства в их центре обработки данных.

Чтобы предотвратить дальнейшее распространение атаки, компания отключила свои системы, что лишило некоторых сотрудников возможности выполнять свою работу.

UL посоветовал сотрудникам не связываться с злоумышленниками и не посещать какие-либо сайты, связанные с операцией вымогателя.

По словам источника, знакомого с атакой, UL решила не платить выкуп и вместо этого восстанавливает данные из резервных копий.

Поскольку для восстановления устройств требуется время, атака привела к тому, что клиентский портал myUL оставался в автономном режиме, пока они восстанавливаются…

«UL обнаружила необычную активность в своих системах 13 февраля 2021 года и немедленно приняла меры предосторожности, чтобы исправить ситуацию, в том числе отключила системы, привлекла ведущую фирму по кибербезопасности, чтобы помочь нам провести расследование и уведомить соответствующие органы. Нашей первоочередной задачей является восстановление наших систем, чтобы свести к минимуму любые перебои в работе наших клиентов».

«Пока мы не узнаем больше из нашего расследования, мы не можем строить предположения относительно типа информации, которая может быть потенциально затронута. Если мы определим, что данные затронуты, мы предпримем соответствующие действия», - UL LLC

Неизвестно, какая операция-вымогатель провела атаку и похитила ли она незашифрованные файлы.

Поскольку большинство программ-вымогателей, нацеленных на предприятия, крадут незашифрованные файлы для использования в стратегии двойного вымогательства, банда вымогателей, вероятно, украла данные во время атаки». ***(Lawrence Abrams. Underwriters Laboratories (UL) certification giant hit by ransomware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/underwriters-laboratories-ul-certification-giant-hit-by-ransomware/). 19.02.2021).***

***

«Французская страховая компания Mutuelle Nationale des Hospitaliers (MNH) подверглась атаке с использованием программ-вымогателей, серьезно нарушивших работу компании. BleepingComputer узнал.

MNH - первая компания взаимного страхования во Франции, которая предоставляет услуги медицинского страхования, и планы ее деятельности ориентированы на сектор здравоохранения.

Веб-сайт компании используется участниками для составления страховых котировок или для управления услугами и льготами.

После атаки на сайте mnh.fr отображается уведомление о том, что он подвергся кибератаке, начавшейся 5 февраля. В результате этой атаки их веб-сайты и телефонная платформа стали недоступны.

«MNH подвергается кибератаке с пятницы, 5 февраля 2021 года. Компьютерные системы были отключены по соображениям безопасности.

«Наши веб-сайты (mnh.fr, зона для участников, соответствующие и избранные экстранеты), а также наша телефонная платформа (3031) временно недоступны. Время обработки ваших запросов увеличено», - заявил Жерар Вюдепот, генеральный директор MNH, уведомление на сайте MNH.

Два дня назад независимый исследователь безопасности поделился веб-страницей Tor с BleepingComputer, которая действует как страница переговоров о выкупе для атаки MNH.

Страница связана с сайтом mnh.fr и определяет, как злоумышленники будут вести переговоры с компанией. Он также советует MNH использовать учетную запись protonmail во время переговоров и не связываться с полицией, иначе полиция конфискует их банковские счета.

Сайт предлагает возможность отправить банде программ-вымогателей одно электронное письмо, чтобы начать переговоры и выполнить тестовое дешифрование одного файла.

Этот сайт Tor принадлежит вымогателю RansomExx, переименованной версии вымогателя Defray777.

Хотя эта группа программ-вымогателей действует с 2018 года, она стала намного более активной в июне 2020 года, когда она переименовалась в RansomExx и начала нацеливаться на крупные организации.

Как и другие операции с программами-вымогателями, управляемыми человеком, RansomExx скомпрометирует сеть и начнет собирать незашифрованные файлы для попыток вымогательства.

Получив доступ к паролю администратора, они развертывают программу-вымогатель в сети и шифруют все ее устройства.

В отличие от большинства других программ-вымогателей, RansomExx также создал версию для Linux, чтобы гарантировать, что они могут быть нацелены на все важные серверы и данные в организации.

Некоторые из громких атак банды RansomExx в прошлом включают правительственные сети Бразилии, Департамент транспорта Техаса (TxDOT), Konica Minolta, IPG Photonics и Tyler Technologies.

BleepingComputer попытался связаться с MNH по поводу этой атаки, но не получил ответа». ***(Lawrence Abrams. French MNH health insurance company hit by RansomExx ransomware // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/french-mnh-health-insurance-company-hit-by-ransomexx-ransomware/). 10.02.2021).***

***

«Centrais Eletricas Brasileiras (Eletrobras) и Companhia Paranaense de Energia (Copel), две крупные электроэнергетические компании в Бразилии, объявили, что за последнюю неделю они подверглись атакам программ-вымогателей.

Контролируемые государством, оба являются ключевыми игроками в стране. Copel является крупнейшей в штате Парана, а Eletrobras - крупнейшей энергокомпанией в Латинской Америке, а также владеет Eletronuclear, дочерней компанией, занимающейся строительством и эксплуатацией атомных электростанций.

Обе атаки программ-вымогателей нарушили работу и вынудили компании приостановить работу некоторых своих систем, по крайней мере, временно.

Атомные станции не пострадали

В случае с Eletrobras инцидент произошел в ее дочерней компании Eletronuclear и был классифицирован как атака с использованием вымогателя. Он затронул некоторые административные серверы сети и не повлиял на работу атомных электростанций Angra 1 и Angra 2.

Операции на двух станциях отключены от административной сети по очевидным причинам безопасности, поэтому подача электроэнергии в Национальную межсетевую систему не пострадала, говорится в сообщении компании в среду.

Обнаружив атаку, Eletronuclear приостановила работу некоторых своих систем для защиты целостности сети. Вместе с командой управляемых служб безопасности компания изолировала вредоносное ПО и ограничила последствия атаки.

В уведомлении мало деталей и не уточняется, является ли атака также утечкой данных, поскольку операторы программ-вымогателей часто крадут данные из сети жертвы перед развертыванием процедуры шифрования.

Впереди утечка копеля

В случае Copel атака является делом рук банды вымогателей Darkside, которая утверждает, что украла более 1000 ГБ данных и что в кеше содержится конфиденциальная информация о доступе к инфраструктуре и личные данные высшего руководства и клиентов.

По словам хакеров, они получили доступ к решению CyberArk компании для управления привилегированным доступом и перехватили пароли в открытом виде через локальную и интернет-инфраструктуру Copel.

Помимо этого, Darkside сообщает, что у них есть более 1000 ГБ конфиденциальных данных, принадлежащих Copel, которые содержат карты сети, схемы и расписания резервного копирования, доменные зоны для основного сайта Copel и домен интрасети.

Они также утверждают, что отфильтровали базу данных, в которой хранятся данные Active Directory (AD) - файл NTDS.dit, который включает информацию об объектах пользователей, группах, членстве в группах и хэшах паролей для всех пользователей в домене.

Хотя в базе данных AD нет паролей в виде обычного текста, существуют инструменты, которые могут взламывать хэши в автономном режиме или использовать их в так называемых атаках с передачей хэша, где они действуют как сам пароль.

В отличие от других операторов программ-вымогателей, Darkside не предоставляет украденные данные на своих сайтах утечки. Вместо этого они создали распределенную систему хранения, чтобы разместить ее в течение шести месяцев.

Доступ к этим тайникам проверяется членами банды. Это означает, что, хотя данные Copel не находятся в свободном доступе, третьи стороны, включая хакеров, могут легко их получить.

Основные системы целы

Copel - крупнейшая компания в штате Парана, а также первая бразильская компания электроэнергетического сектора, котирующаяся на Нью-Йоркской фондовой бирже.

Дата вторжения остается нераскрытой, но Copel объявил об инциденте в документации, поданной в Комиссию по ценным бумагам и биржам (SEC) в понедельник, 1 февраля.

Компания обнаружила атаку и немедленно приняла меры, чтобы остановить ее распространение по сети. Было начато расследование для определения всех последствий атаки.

Что можно сказать наверняка, так это то, что основные системы остались нетронутыми, а электроснабжение и телекоммуникационные услуги продолжали нормально функционировать.

«Системы управления и защиты обнаружили атаки, и компания немедленно выполнила протоколы безопасности, в том числе приостановила работу своей

компьютеризированной среды для защиты целостности информации. Полная оценка произошедшего продолжается, и Компания предпринимает необходимые шаги для восстановления нормального режима» - Копель.

Неясно, сколько сегментов сети Copel подверглось атаке и смогли ли хакеры развернуть процедуру шифрования. BleepingComputer обратился к Copel с просьбой о комментариях, и мы обновим статью, когда появится официальное заявление». ***(Ionut Ilascu. Eletrobras, Copel energy companies hit by ransomware attacks // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/eletrobras-copel-energy-companies-hit-by-ransomware-attacks/). 05.02.2021).***

***

«Операция вымогателя Ziggy была закрыта и выпустила ключи дешифрования жертв после опасений по поводу недавних действий правоохранительных органов и вины за шифрование жертв.

В минувшие выходные исследователь безопасности М. Шахпасанди сообщил BleepingComputer, что администратор Ziggy Ransomware объявил в Telegram, что они прекращают работу и будут выпускать все ключи дешифрования.

В интервью BleepingComputer администратор программы-вымогателя сказал, что они создали программу-вымогатель для получения денег, поскольку они живут в «стране третьего мира».

Чувствуя себя виноватым в своих действиях и опасаясь недавних принудительных действий против программ-вымогателей Emotet и Netwalker, администратор решил выключить систему и освободить все ключи.

Сегодня администратор программы-вымогателя Ziggy опубликовал файл SQL, содержащий 922 ключа дешифрования для зашифрованных жертв. Для каждой жертвы в SQL-файле перечислены три ключа, необходимые для расшифровки их зашифрованных файлов.

Администратор вымогателя также разместил дешифратор [VirusTotal], который жертвы могут использовать с ключами, указанными в файле SQL.

Помимо дешифратора и файла SQL, администратор вымогателя поделился исходным кодом другого дешифратора с BleepingComputer, который содержит ключи автономного дешифрования.

При заражении программами-вымогателями используются автономные ключи дешифрования для расшифровки зараженных жертв, которые не были подключены к Интернету или командный сервер был недоступен.

Администратор программы-вымогателя также поделился этими файлами с экспертом по программам-вымогателям Майклом Гиллеспи, который создал дешифратор для Ziggy Ransomware, используя выпущенные ключи.

Хотя администратор программы-вымогателя, кажется, честен в своем намерении завершить работу и освободить ключи, BleepingComputer всегда предлагает использовать дешифратор компании безопасности, а не тот, который предоставлен злоумышленником.

"Предоставление ключей, добровольно или невольно, является наилучшим возможным результатом. Это означает, что прошлые жертвы могут восстановить

свои данные без необходимости платить выкуп или использовать дешифратор разработчика, который может содержать бэкдор и / или ошибки. И, конечно, это также означает, что нужно беспокоиться на одну группу программ-вымогателей меньше».

«Недавний арест лиц, связанных с операцией Emotet и Netwalker, может вызвать у некоторых актеров холодные ноги. Если это так, мы вполне можем увидеть, как больше групп прекращают операции и передают свои ключи. Скрестив пальцы, - сказал BleepingComputer Бретт Кэллоу из Emsisoft.

На прошлой неделе программа- вымогатель Fonix также отключилась и выпустила ключи и дешифратор. Администратор Ziggy сказал BleepingComputer, что они дружат с группой вымогателей Fonix и из той же страны». ***(Lawrence Abrams. Ziggy ransomware shuts down and releases victims' decryption keys // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ziggy-ransomware-shuts-down-and-releases-victims-decryption-keys/). 07.02.2021).***

***

«Все больше и больше жертв программ-вымогателей сопротивляются вымогателям и отказываются платить, когда они могут восстановить данные из резервных копий, несмотря на угрозы хакеров по утечке данных, украденных до шифрования.

Такая позиция привела к тому, что в четвертом квартале 2020 года средний размер выкупа значительно снизился по сравнению с предыдущим кварталом, сообщает компания Coveware, занимающаяся защитой от программ-вымогателей.

Но есть еще более коварный феномен, когда данные уничтожаются в результате атаки, и у компаний нет возможности восстановить их, даже если они заплатят выкуп.

Атаки программ-вымогателей с удалением данных

В последнем квартале 2020 года Coveware получила все большее количество отчетов о целых кластерах серверов и общих данных, уничтоженных в результате атак программ-вымогателей.

Обычно атаки программ-вымогателей нацелены на системы резервного копирования и шифруют дорогостоящие машины. Однако в этих случаях восстанавливать было нечего, и жертвам приходилось восстанавливать системы.

Злоумышленники, делающие это намеренно, не имеют особого смысла, поскольку полагаются на файлы, доступные в зашифрованном состоянии; в противном случае у жертв не было бы причин платить за средство дешифрования.

«Рост случайного уничтожения данных привел к тому, что некоторые жертвы столкнулись с серьезной потерей данных и продолжительными перерывами в работе, поскольку они изо всех сил пытались восстановить системы с нуля» - Coveware.

Эти инциденты могут быть следствием того, что менее квалифицированные злоумышленники наводняют бизнес-сцену, посвященную программам-вымогателям, и что-то не так. Coveware не исключает, что эта тенденция может сохраниться и в этом году.

Если первая из приведенных выше теорий верна, то неправильно обработанные атаки могут быть результатом деятельности филиалов открытых операций «программа-вымогатель как услуга» (RaaS), которые не устанавливают стандарт принятия; или хакеров, не связанных с аффилированными лицами, которые проводят кампании без помощи за пределами своей небольшой группы.

Меньшие требования выкупа

Угроза жертвам утечкой украденных данных с целью заставить их заплатить - это поворот, который теперь закрытая операция вымогателя Maze представила в конце 2019 года.

Другие банды, работающие в сфере программ-вымогателей, видя потенциал для более высокой прибыли от этой тактики двойного вымогательства, последовали их примеру и создали так называемые «сайты утечек», где публикуют данные, украденные у жертв, которые не заплатили выкуп.

Не имея никакой другой гарантии, кроме заявления злоумышленников о том, что украденные данные не будут опубликованы, компании-жертвы уступили и действовали, выплачивая выкуп.

Статистика Coveware, похоже, указывает на то, что этот метод потерял часть своей силы, поскольку средний спрос на выкуп упал на 34% в четвертом квартале 2020 года. В пересчете на наличные деньги он резко вырос с 233 817 долларов до 154 108 долларов.

Если посмотреть на медианное значение, то падение будет более глубоким: со 110 532 до 49 450 долларов на 55%. Coveware заявляет, что это «резкое сокращение объясняется тем, что большее количество жертв атак с кражей данных говорят «ДОСТАТОЧНО» и предпочитают не платить».

Это происходит на фоне увеличения числа атак программ-вымогателей в четвертом квартале, сопровождаемых угрозой утечки украденных данных, от 50% до 70%.

Компании правы, не доверяя хакерам удаление украденных данных, если им заплатили, поскольку Coveware продолжает видеть признаки того, что это происходит не во всех случаях.

Более того, некоторые банды лгут о похищении данных и фабрикации «улик» только для того, чтобы усилить давление на жертву утечки данных и принудить к выплате.

Coveware советует жертвам программ-вымогателей не платить хакерам. Если они это сделают, нет никакой гарантии, что их данные в безопасности, и вот чего им следует ожидать:

Данные не могут быть достоверно уничтожены злоумышленником. Жертвы должны предположить, что он может быть продан, продан, потерян или задержан для второй / будущей попытки вымогательства.

Хранение украденных данных осуществлялось несколькими сторонами и не защищалось. Даже если злоумышленник удаляет объем данных после платежа, другие стороны, имевшие к нему доступ, могли сделать копии, чтобы они могли вымогать у жертвы в будущем.

Данные могут быть преднамеренно или ошибочно опубликованы в любом случае до того, как жертва сможет ответить на попытку вымогательства.

Злоумышленник может не предоставить полные записи о том, что было похищено, даже если они явно обещают предоставить такие артефакты после оплаты.

Хотя средний и средний размер выкупа резко снизился за последние четыре месяца, известные операторы программ-вымогателей продолжают собирать большие деньги с тщательно отобранных жертв.

Согласно статистике Coveware, закрытые операции RaaS, такие как Sodinokibi, Egregor и Ryuk, доминируют на рынке, взламывая компании в основном с помощью фишинга и взломанных соединений RDP.

Следующим в списке идет Netwalker, одному из филиалов которого предъявлено обвинение в США, а его темные веб-сайты изъяты правоохранительными органами, за ним следует Maze, который теряет свое место из-за недавнего закрытия.

В конце прошлого года в первую десятку списка Coveware вошли новые штаммы вымогателей, такие как Conti, Suncrypt, Zeppelin, MedusaLocker. Некоторые из них, скорее всего, вскоре увеличат активность». ***(Ionut Ilascu. Ransomware attacks increasingly destroy victims' data by mistake // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ransomware-attacks-increasingly-destroy-victims-data-by-mistake/). 04.02.2021).***

***

«Операция вымогателя Babyk запустила новый сайт утечки данных, который используется для публикации украденных данных жертвы в рамках стратегии двойного вымогательства. Включен список целей, которые они не будут атаковать, с некоторыми исключениями, которые определенно выделяются.

В 2019 году программа-вымогатель Maze представила новую стратегию двойного вымогательства, заключающуюся в краже незашифрованных файлов с последующей угрозой публичного размещения их на сайтах утечки данных, если выкуп не будет уплачен.

Вскоре после этого другие банды программ-вымогателей приняли эту стратегию, пока она не стала популярным методом вымогательства у злоумышленников.

Babyk запускает сайт утечки данных

Программа-вымогатель Babyk, также известная как Babuk, - это новая программа-вымогатель, запущенная в начале года и нацеленная на корпоративные организации по всему миру.

При первом запуске банда вымогателей слила свои данные в сообщениях на хакерском форуме Raid Forums, но заявила, что планировала запустить специальный сайт утечки.

Исследователь безопасности Emsisoft Бретт Кэллоу поделился новым сайтом, недавно созданным группой Babyk Ransomware, где они в настоящее время перечисляют четырех жертв и просочившиеся данные о трех из них.

На сайте утечки данных есть список организаций, которые они не будут шифровать, в том числе больницы, некоммерческие организации, школы и малые предприятия.

Для каждой из этих категорий банды вымогателей перечисляют следующие исключения:

Мы не проводим аудит следующих категорий организаций

Больницы: кроме частных клиник пластической хирургии, частных стоматологических клиник.

Некоммерческая организация: любой некоммерческий благотворительный фонд (кроме фондов, которые помогают ЛГБТ и BLM).

Школы: кроме крупных университетов

Малый бизнес: компании с годовой выручкой менее 4 млн $ (информацию о выручке мы получаем от zoominfo)

В прошлом BleepingComputer исключалась из сферы здравоохранения и того, что участники программ-вымогателей называют «социально важными» службами, такими как служба экстренной помощи, приюты и дома престарелых.

Исключения для некоммерческих организаций - это первый раз, когда BleepingComputer увидела, что личное мнение определяет, будет ли операция вымогателя шифровать организацию.

С открытием сайта Бабука в настоящее время насчитывается девяносто активных сайтов утечки данных программ-вымогателей, используемых в тактике двойного вымогательства». ***(Lawrence Abrams. Babyk Ransomware won't hit charities, unless they support LGBT, BLM // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/babyk-ransomware-wont-hit-charities-unless-they-support-lgbt-blm/). 02.02.2021).***

***

«Недавняя кибератака, вынудившая Голландский исследовательский совет (NWO) отключить свои серверы и приостановить процессы распределения грантов, была вызвана бандой вымогателей DoppelPaymer.

Хакеры получили доступ к сети NWO 8 февраля и украли внутренние документы, угрожая утечкой их, если организация не заплатит выкуп.

Ни копейки ДоппельПаймер

Поскольку NWO не сотрудничает с киберпреступниками, DoppelPaymer опубликовал доказательства кражи внутренних данных на своем сайте утечки. Эта тактика типична для банд программ-вымогателей, и ее цель - заставить жертву заплатить выкуп.

NWO - это основная организация, которая финансирует исследователей в университетах и институтах Нидерландов, делая ежегодные инвестиции в размере до одного миллиарда евро.

14 февраля организация объявила, что ее сеть была взломана, не сообщив подробностей инцидента, а только о влиянии, которое она оказывает на ее деятельность.

В среду банда вымогателей DoppelPaymer слила дюжину файлов, украденных с серверов NWO, чтобы показать, что у них больший кеш и они все еще открыты для переговоров.

[Хотя банда программ-вымогателей называет себя Dopple, средства массовой информации называют этого актера Doppel из-за «доппелированного» расширения, которое они добавляют к зашифрованным файлам в системе жертвы]

В обновлении об инциденте вчера, организация говорит, что хакеры имеют внутренние СВЫ документы прошлых лет, которые включают сведения о своих сотрудниках. Это не меняет его решения не платить хакерам.

Восстановление сети

NWO в настоящее время работает над восстановлением сети, что указывает на то, что системы были зашифрованы, что типично для большинства участников программ-вымогателей. Ожидается, что операции возобновятся через несколько недель.

В FAQ от организации сообщается, что кибератака затронула сетевые диски с данными, обработанными NWO, офисом NWO-I, Национальным управляющим органом по практическим исследованиям SIA и Нидерландской инициативой исследований в области образования (NRO).

Другие организации, использующие те же сетевые серверы, - это NRO Steering Body, SIA Steering Body, TKI-HTSM, TKI Chemie, European Polar Board и LNVH.

Британское агентство исследований и инноваций (UKRI), которое выполняет ту же миссию, что и NWO, в январе также подверглось атаке с использованием программ-вымогателей, в результате которых были зашифрованы данные и затронуты некоторые из его сервисов.

Хотя NWO еще предстоит проделать определенную работу по восстановлению услуг и операций, UKRI объявила о восстановлении услуг, предоставляемых ее британским исследовательским офисом (UKRO), базирующимся в Брюсселе. Пользователи должны будут сбросить свои пароли при входе в систему». ***(Ionut Ilascu. Dutch Research Council (NWO) confirms ransomware attack, data leak // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/dutch-research-council-nwo-confirms-ransomware-attack-data-leak/). 25.02.2021).***

***

«Французское национальное агентство по кибербезопасности обнаружило новый вариант программы-вымогателя Ryuk с похожими на червя возможностями, которые позволяют ему распространяться на другие устройства в локальных сетях жертв, во время расследования атаки в начале 2021 года.

«Благодаря использованию запланированных задач вредоносное ПО распространяется - с машины на машину - в домене Windows», - говорится в опубликованном сегодня отчете ANSSI (сокращение от Agence Nationale de la Sécurité des Systèmes d'Information).

«После запуска он будет распространяться на каждую доступную машину, на которой возможен доступ к Windows RPC».

Саморепликация на другие сетевые устройства

Для распространения по локальной сети новый вариант Ryuk перечисляет все IP-адреса в локальном кэше ARP и отправляет то, что выглядит как пакеты Wake-on-LAN (WOL), на каждое из обнаруженных устройств. Затем он монтирует все общие ресурсы, найденные для каждого устройства, чтобы можно было зашифровать содержимое.

Возможность Ryuk монтировать и шифровать диски удаленных компьютеров ранее наблюдалась генеральным директором Advanced Intelligence Виталием Кремезом в прошлом году.

Что отличает этот новый образец Ryuk от других, так это его способность копировать себя на другие устройства Windows в локальных сетях жертв.

Кроме того, он может выполнять себя удаленно, используя запланированные задачи, созданные на каждом впоследствии скомпрометированном сетевом узле с помощью законного инструмента schtasks.exe для Windows…

Несмотря на то, что он не использует механизм исключения, который предотвратил бы повторное шифрование устройств, ANSSI говорит, что новый вариант все еще может быть заблокирован от заражения других хостов в сети путем изменения пароля учетной записи привилегированного домена, которую он использует для распространения на другие хосты.

«Одним из способов решения проблемы может быть изменение пароля или отключение учетной записи пользователя (в соответствии с используемой учетной записью), а затем переход к двойному изменению пароля домена KRBTGT», - сказал ANSSI.

«Это вызовет множество нарушений в домене и, скорее всего, потребует множества перезагрузок, но также немедленно остановит распространение. Также можно рассмотреть другие подходы к сдерживанию распространения, особенно через нацеливание на среду выполнения вредоносного ПО».

Индикаторы компрометации (IOC), связанные с этим новым вариантом Ryuk, можно найти здесь.

Банда вымогателей Ryuk

Ryuk - это группа программ-вымогателей как услуги (RaaS), впервые обнаруженная в августе 2018 года и оставшая после себя длинный список жертв.

Банды RaaS известны своими частными партнерскими программами, в которых партнеры могут подавать заявки и резюме для подачи заявки на членство.

Ryuk находится на вершине рейтинга RaaS, его полезные нагрузки были обнаружены примерно в каждой третьей атаке программ-вымогателей за последний год.

Группа доставляет полезные нагрузки в рамках многоэтапных атак, используя векторы заражения Emote t, BazarLoader или TrickBot для быстрого проникновения в сети своих целей.

Филиалы Ryuk стояли за массой атак на систему здравоохранения США, начиная с ноября 2020 года. Обычно они просят огромные выкуп, собрав 34 миллиона долларов всего с одной жертвы в прошлом году.

Проследив за денежным оборотом жертв программ-вымогателей Ryuk, исследователи из компаний по анализу угроз Advanced Intelligence и HYAS оценили, что операция RaaS принесла не менее 150 миллионов долларов.

В течение третьего квартала 2020 года аффилированные лица Ryuk еженедельно поражали в среднем около 20 компаний». ***(Sergiu Gatlan. Ryuk ransomware now self-spreads to other Windows LAN devices // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ryuk-ransomware-now-self-spreads-to-other-windows-lan-devices/). 26.02.2021).***

***

«Производитель бизнес-джетов Bombardier - последняя компания, которая пострадала от утечки данных со стороны банды вымогателей Clop после того, как злоумышленники использовали уязвимость нулевого дня для кражи данных компании.

Bombardier - один из ведущих мировых производителей бизнес-джетов, в котором работает 16 000 человек, и выручка в 2020 году составила 6,5 миллиардов долларов.

На этой неделе вымогатель Clop разместил файлы, украденные у Bombardier, на своем сайте утечки данных. Эти данные включают в себя проектные схемы самолета и деталей, а также отчеты о летных испытаниях.

Вскоре после того, как BleepingComputer связался с компанией по поводу утечки данных, Bombardier выпустила пресс-релиз, в котором говорилось, что они пострадали от взлома после того, как хакеры украли данные из их «приложения для передачи файлов».

«Первоначальное расследование показало, что неавторизованная сторона получила доступ к данным и извлекла их, воспользовавшись уязвимостью стороннего приложения для передачи файлов, которое работало на специально созданных серверах, изолированных от основной ИТ-сети Bombardier», - сообщил Bombardier.

В последующем электронном письме с Bombardier авиационная компания подтвердила BleepingComputer, что приложение для передачи файлов, на которое они ссылаются, является Accellion FTA. Это приложение для безопасного обмена файлами было вовлечено в серию утечек данных с декабря 2020 года.

В рамках этой атаки Bombardier заявляет, что злоумышленники украли личные и конфиденциальные данные сотрудников, клиентов и поставщиков.

«Судебно-медицинский анализ показал, что была скомпрометирована личная и другая конфиденциальная информация, касающаяся сотрудников, клиентов и поставщиков. Пострадало примерно 130 сотрудников, расположенных в Коста-Рике. Bombardier активно связывалась с клиентами и другими внешними заинтересованными сторонами, чьи данные были потенциально скомпрометированы», - говорит Бомбардье в кибербезопасность нарушение совещательным.

Компания подчеркивает, что серверы Accellion FTA изолированы от остальной сети и злоумышленники не получили доступа к каким-либо другим системам.

Использована уязвимость нулевого дня в Accellion FTA

Accellion FTA - это устаревшая 20-летняя служба передачи файлов, используемая организациями для безопасного обмена конфиденциальными файлами с людьми за пределами своей организации.

В декабре злоумышленник начал использовать уязвимость нулевого дня в устройствах Accellion FTA, которая позволила им украсть данные, хранящиеся на серверах.

Когда Accellion узнал о злоумышленниках, они выпустили обновление безопасности на Рождество, но к тому моменту злоумышленники уже взломали серверы многих организаций и украли данные.

Начиная с февраля, банда вымогателей Clop начала публиковать данные о жертвах, чьи устройства Accellion FTA были взломаны. На сайте утечки данных Клопа произошла утечка таких компаний, как Singtel, Jones Day, Fugro, Danaher и ABS Group.

Известно, что другие компании были взломаны, но не получили утечки данных. К этим компаниям относятся гигант супермаркетов Kroger, Медицинский исследовательский институт QIMR Berghofer, Резервный банк Новой Зеландии, Австралийская комиссия по ценным бумагам и инвестициям (ASIC) и Управление аудитора штата Вашингтон (SAO).

С тех пор, как в декабре начались атаки на устройства Accellion FTA, BleepingComputer изучает утечки данных, и компании сообщили, что они получили записки о выкупе от банды вымогателей Clop.

Эти записки о выкупе не были оставлены в системе, как атака программы-вымогателя, а были отправлены по электронной почте сотрудникам компании.

Ранее на этой неделе отчет компании по реагированию на инциденты Mandiant подтвердил наши подозрения, что злоумышленники, связанные с бандой вымогателей Clop, несут ответственность за атаки на устройства Accellion FTA.

Неясно, провела ли банда вымогателей Clop атаку самостоятельно или другая хакерская группа объединилась с ними, чтобы использовать их сайт утечки данных.

Тем не менее, BleepingComputer может подтвердить, что в начале этого месяца с нами связалась непосредственно банда вымогателей Clop, чтобы предупредить нас о публикации этих нарушений на их сайте.

Мы должны ожидать, что по мере того, как банда вымогателей Clop публикует новые украденные данные на своем веб-сайте, мы увидим больше случаев нарушения данных Accellion FTA». ***(Lawrence Abrams. Ransomware gang extorts jet maker Bombardier after Accellion breach // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/ransomware-gang-extorts-jet-maker-bombardier-after-accellion-breach/). 24.02.2021).***

***

«Группы, похожие на мафию», вероятно, стоят за серией недавних атак с использованием программ-вымогателей, нацеленных на французские больницы, заявил сегодня министр цифровых технологий страны Седрик О.

Отвечая на вопрос на France 2 о недавних атаках, парализовавших ИТ-системы некоторых больниц, О сказал, что за ними «стояли, по всей видимости, не

иностранные державы, а мафиозные группы, часто, но не исключительно из стран Восточной Европы, ищущие деньги.»

9 февраля госпиталь Дакс на юго-западе Франции подвергся атаке программы-вымогателя, в результате которой были зашифрованы ее данные, и персонал вынужден был прибегать к помощи ручки и бумаги. 15 февраля аналогичное нападение произошло в больнице в Вильфранш-сюр-Сон, недалеко от Лиона. Нападения использовали RYUK вымогатель, который предназначен для блокировки компьютерных систем, с хакерами требуя выкуп в обмен на разблокирование их.

Президент Франции Эммануэль Макрон на прошлой неделе пообещал усилить поддержку индустрии кибербезопасности в ответ на атаки.

В своем интервью О сказал, что в настоящее время нет никаких указаний на то, что какие-либо данные были украдены во время атак, но «произошли очень конкретные и серьезные вещи». Отделения неотложной помощи больниц были вынуждены прекратить прием новых пациентов, а их службы медицинской визуализации и телефонные сети вышли из строя.

Министр цифровых технологий также прокомментировал еще один инцидент, связанный с кибербезопасностью в сфере здравоохранения: утечка данных о пациентах из сети биомедицинских лабораторий, затронувшая 500000 пациентов. Компания и орган по защите данных Франции поддерживали контакт, но, похоже, компания не уведомила пациентов, сказал О». ***(JULES DARMANIN. 'Mafia-like groups' behind hospital cyberattacks, French digital minister says // POLITICO (https://www.politico.eu/article/mafia-like-groups-behind-hospital-cyberattacks-french-digital-minister-says/). 25.02.2021).***

***

«TietoEVRY был вынужден закрыть службы и инфраструктуру, поскольку компания продолжает расследование инцидента с соответствующими органами.

Крупный финский ИТ-провайдер подвергся атаке с использованием программ-вымогателей, в результате чего компания вынуждена была отключить некоторые службы и инфраструктуру, что привело к сбоям в работе клиентов, пока компания принимает меры по восстановлению.

Норвежский деловой журнал E24 сообщил о нападении на финскую компанию TietoEVRY в Эспоо во вторник, утверждая, что разговаривал с Гейром Ремманом, директором по коммуникациям компании. Ремман признал технические проблемы с несколькими услугами, которые TietoEVRY предоставляет 25 клиентам, которые, как говорится в отчете, возникли «из-за атаки с целью выкупа».

Ремман сказал E24, что компания считает нападение «серьезным преступным деянием». TietoEVRY отключил неуказанные службы и затронутую инфраструктуру «в качестве превентивной меры», пока не сможет восстановить соответствующие данные, и перезапустить системы «контролируемым образом», - сказал он.

Однако в настоящее время не похоже, что злоумышленники получили доступ к каким-либо важным или личным данным или были украдены, добавил Ремман.

TietoEVRY - компания, занимающаяся разработкой программного обеспечения и услуг, предоставляющая ИТ-услуги и услуги по разработке продуктов в 20 странах. Акционерная компания котируется на фондовых биржах NASDAQ OMX в Хельсинки и Стокгольме.

Согласно отчету, компания проинформировала клиентов об инциденте и постоянно поддерживает с ними связь по мере развития ситуации.

«TietoEVRY очень серьезно относится к этому инциденту и приносит извинения за неудобства, которые он причиняет нашим клиентам», - сказал Кристиан Педерсен, управляющий партнер Tietoevry, Норвегия, в заявлении для СМИ. «Мы привлекли расширенную команду с необходимыми возможностями и компетенциями и работаем с соответствующими партнерами, чтобы справиться с ситуацией».

Согласно отчету Реммана, в число этих партнеров входят Управление национальной безопасности (NSM) и NorCert, агентства в Финляндии, которые занимаются кибератаками, с которыми TietoEVRY немедленно связался после атаки.

«Мы ведем диалог с полицией по этому делу», - сказал он E24. «В то же время мы рекомендуем клиентам также сообщать о случившемся в полицию».

NSM Финляндии подтвердило, что TietoEVRY связывался с ним и что агентство поддерживает компанию в смягчении последствий и расследовании инцидента, чтобы «выяснить, использовалось ли подобное вредоносное ПО где-либо еще», - сообщила СМИ пресс-секретарь Мона Стрем Арнёй. По ее словам, NSM также поможет компании восстановить инфраструктуру.

Сарью Найяр, генеральный директор Gurucul, отметил, что большинство банд вымогателей недоступны для правоохранительных органов.

«Хотя финская ИТ-компания TietoEVRY сможет эффективно вылечиться, маловероятно, что она добьется справедливости даже после привлечения соответствующих правоохранительных органов», - сказала она Threatpost. «Многие из этих киберпреступных группировок имеют международный масштаб и действуют из регионов, которые закрывают глаза на преступления против иностранных объектов, если не молча поддерживают их деятельность. Это усложняет работу правоохранительных органов и ложится дополнительным бременем на организации по поддержанию их собственной защиты в актуальном состоянии и ее эффективности».

В настоящее время неизвестно, какая группа программ-вымогателей несет ответственность за атаку. Некоторые из них были активны в последнее время, в том числе банда вымогателей Clop, которая была связана с недавними глобальными атаками нулевого дня на пользователей устаревшего продукта Accellion File Transfer Appliance; DoppelPaymer, который ударил Kia Motors с нападением, требуя $ 20 млрд в качестве выкупа на прошлой неделе; и HelloKitty, который, как подозревают, стоит за атакой CD Projekt Red, компании по разработке видеоигр, стоящей за Cyberpunk 2077, в начале этого месяца.

«Атаки на TietoEVRY должны стать сигналом для каждого предприятия, имеющего доступ к Интернету: вас сканируют на предмет доступных хостов, открытых сетевых портов, уязвимостей и неправильных конфигураций», - сказал

Threatpost Гаррет Граек, генеральный директор YouAttest. «Хакеры используют возможности. Внедренное вредоносное ПО практически не имеет значения для первой фазы цепочки кибер-убийств (разведка)».

Он добавил: «Как только открытый сервер считается открытым, на сервере / сервисе запускается сканирование уязвимостей, чтобы увидеть, какие вредоносные программы могут быть имплантированы. Это может быть бот для дальнейшего рассылки спама или исследования - или это могут быть трояны, которые продолжают цепочку кибер-убийств и перечисляют вашу среду, повышают свои привилегии и перемещаются по вашему предприятию. Конечным результатом может быть атака программы-вымогателя или кража данных для продажи в темной сети».

TietroEVRY не сразу ответил на электронное письмо Threatpost во вторник с просьбой подтвердить и подробности атаки. Педерсен сказал E24, что компания не публично спекулирует и не раскрывает подробностей, пока не проведет дальнейшее расследование.

Это развивающаяся история». ***(Elizabeth Montalbano. Finnish IT Giant Hit with Ransomware Cyberattack // Threatpost (https://threatpost.com/finnish-it-giant-ransomware-cyberattack/164193/). 23.02.2021).***

***

Програми-трояни

«Новая версия Agent Tesla RAT может блокировать программное обеспечение защиты конечных точек, поддерживаемое Microsoft ASMI.

Исследователи определили новые версии трояна удаленного доступа (RAT) Agent Tesla, нацеленного на антивирусный интерфейс Windows, используемый поставщиками систем безопасности для защиты ПК от атак. В недавно обнаруженных вариантах были также внедрены новые возможности обфускации, что повысило ставки для предприятий, которые могли бы защищаться от постоянно развивающегося вредоносного ПО Agent Tesla.

Главным среди обновлений является то, что вредоносная программа теперь нацелена на программный интерфейс Microsoft для защиты от вредоносных программ (ASMI), чтобы избежать обнаружения. ASMI позволяет приложениям и службам интегрироваться с любым продуктом защиты от вредоносных программ, установленным на машине. Вредоносная программа теперь также имеет дополнительную возможность развертывания клиента Tor для сокрытия своих сообщений, а также использования приложения чата Telegram для эксфильтрации данных.

Исследователи предупреждают, что все эти изменения затрудняют как «песочницу», так и статический анализ, а также обнаружение вредоносных программ на конечных точках.

«Агент Tesla остается постоянной угрозой - в течение многих месяцев он оставался одним из основных семейств вредоносных программ, обнаруженных Sophos», - заявили исследователи Sophos во вторник. «Из-за этого непрерывного

потока атак агента Тесла мы считаем, что вредоносное ПО будет и дальше обновляться и модифицироваться разработчиками, чтобы обходить защиту конечных точек и электронной почты».

Агент Тесла впервые появился на сцене в 2014 году, специализируясь на кейлоггах (предназначенных для записи нажатий клавиш, сделанных пользователем с целью кражи данных, таких как учетные данные и т. Д.) И кражи данных. Агент Тесла исторически приходил во вредоносном спаме в виде вложения.

Первая стадия новой версии вредоносного ПО включает загрузчик на базе.NET. Загрузчик собирает обфусцированный код с таких сайтов, как Pastebin и Hastebin (который позиционирует себя как «альтернатива Pastebin с открытым исходным кодом»). Это не новая тактика, поскольку агент Тесла ранее обращался к законному веб-сервису, подобному Pastebin, для загрузки вредоносных программ.

Затем установщик агента Тесла пытается перезаписать код в Microsoft AMSI. Сначала загрузчик пытается получить адрес памяти AmsiScanBuffer (функция Microsoft, также известная как amsi.h, которая сканирует буфер, заполненный содержимым на наличие вредоносных программ).

Это делается путем вызова amsi.dll Windows с помощью функции Windows LoadLibraryA для получения базового адреса библиотеки DLL. Затем он использует функцию GetProcAddress для получения базового адреса и имени процедуры «AmsiScanBuffer» для получения адреса функции.

Как только агент Tesla получает адрес AmsiScanBuffer, он исправляет первые 8 байтов функции в памяти. По словам исследователей, это заставляет AMSI возвращать ошибку (код 0x80070057), в результате чего все сканирования памяти AMSI кажутся недействительными.

«Это блокирует программное обеспечение для защиты конечных точек с поддержкой AMSI, по сути заставляя их пропускать дальнейшее сканирование AMSI для динамически загружаемых сборок в рамках процесса Agent Tesla», - заявили исследователи. «Поскольку это происходит на ранней стадии выполнения загрузчика первой стадии, он обеспечивает любую защиту AMSI от последующих компонентов загрузчика, загрузчика второй стадии и самой полезной нагрузки агента Tesla».

В новой версии Agent Tesla также добавлены возможности развертывания клиента Tor. По словам исследователей, это бесплатное программное обеспечение с открытым исходным кодом обеспечивает анонимное общение и служит для агента Тесла инструментом для сокрытия своих сообщений.

«Если этот параметр выбран в файле конфигурации, вредоносная программа загружает и устанавливает клиент Tor с официального сайта Tor», - заявили исследователи. Если клиент Tor уже присутствует, он завершает процесс перед установкой нового и записывает файл конфигурации torrc из зашифрованных строк, жестко закодированных во вредоносное ПО».

Новые возможности

Исследователи заявили, что функциональность этих двух новых вариантов в целом одинакова, но теперь они включают обновления собираемых данных и способов их удаления.

В новой версии Agent Telsa разработчики теперь могут захватывать данные из буфера обмена Windows. Буфер обмена Windows - это место для хранения элементов, которые были вырезаны или скопированы; Эти данные могут включать в себя что угодно, от конфиденциальных данных, скопированных из электронных писем или документов, до паролей. Затем эти данные отправляются обратно на командно-управляющий (C2) сервер.

Еще одно отличие состоит в том, что в новой версии Agent Tesla количество приложений, предназначенных для сбора учетных данных, «значительно увеличено».

Агент Tesla ранее нацелился на учетные данные из таких приложений, как Apple Safari, Chromium, Google Chrome, Iridium, Microsoft IE и Edge, Mozilla Firefox, Mozilla Thunderbird, OpenVPN, Opera, Opera Mail, Qualcomm Eudora, Tencent QQBrowser и Яндекс. Вредоносная программа теперь также нацелена на FTPNavigator (Интернет-приложение для Windows, которое упрощает передачу по FTP), WinVNC4 (средство управления удаленным рабочим столом, позволяющее пользователям управлять компьютерами удаленно), WinSCP (обеспечивающее безопасную передачу файлов между локальным и удаленным компьютерами) и SmartFTP (программа для передачи файлов по сети для Microsoft).

«Функция кражи учетных данных также включает в себя код, который запускает отдельный поток для эксфильтрации файлов cookie браузера. Хотя этот код присутствует во всех образцах Agent Tesla как из v2, так и из v3, он не всегда используется», - заявили исследователи. «Кроме того, эта функция не устанавливается в файле конфигурации, поэтому, возможно, злоумышленники должны приобрести эту премиальную функцию у разработчика агента Тесла».

В то время как агент Tesla ранее общался с сервером C2 через HTTP, SMTP (простой протокол передачи почты) и FTP (протокол передачи файлов), новая версия также использует Telegram для эксфильтрации данных, отправляя украденные данные в частный чат Telegram.

Агент Тесла: угроза через семь лет

Хотя троян удаленного доступа (RAT) агента Tesla, нацеленный на Windows, был активен более семи лет, исследователи заявили, что они продолжают видеть новые варианты вредоносного ПО в растущем количестве атак за последние 10 месяцев по сравнению с печально известным например, вредоносное ПО TrickBot или Emotet.

Фактически, в декабре 2020 года на агент Tesla приходилось 20 процентов вредоносных вложений электронной почты, обнаруженных в телеметрии исследователей.

Исследователи считают, что агент Тесла продолжит развиваться.

«Различия между ними демонстрируют, как RAT развивалась, используя несколько типов обхода защиты и обфускации, чтобы избежать обнаружения», - сказали они». ***(Lindsey O'Donnell. Agent Tesla Trojan 'Kneecaps' Microsoft's Anti-Malware Interface // Threatpost (https://threatpost.com/agent-tesla-microsoft-asmi/163581/). 02.02.2021).***

***

«Официальные лица Малайзии объявили в четверг об аресте 11 подозреваемых, которые, как считается, являются частью группы хактивистов, которая в конце января испортила правительственные веб-сайты.

Согласно сообщениям, опубликованным на странице Facebook в начале этого месяца, группа, называющая себя Anonymous Malaysia, испортила 17 веб-сайтов местных органов власти и университетов.

Дефейсы были частью кампании, которую группа назвала # OpsWakeUp21, в ходе которой они хотели подчеркнуть низкую безопасность правительственных веб-сайтов, разместив предупреждающие сообщения на своих первых страницах (см. Снимок экрана выше).

Власти Малайзии начали расследование после того, как теракты произошли в конце января, и в среду были арестованы 11 подозреваемых.

Согласно местным сообщениям, подозреваемые были в возрасте от 22 до 40 лет из регионов Паханг, Джохор, Перак и долина Кланг.

О ПОДОБНОЙ АКТИВНОСТИ ХАКТИВИЗМА СООБЩАЕТСЯ В МЬЯНМЕ

Аресты произошли после того, как ранее на этой неделе другая группа хактивистов, названная Myanmar Hackers, испортила сайты для военных Мьянмы, государственной телекомпании MRTV, Центрального банка, Управления порта, Управления по санитарному надзору за качеством пищевых продуктов и медикаментов и местных правоохранительных органов.

Кибернетические вторжения и искажения веб-сайтов были частью общенациональных протестов против нынешнего правительства, которое в начале этого месяца незаконно захватило власть после военного переворота.

1 февраля военное руководство Мьянмы приказало арестовать членов партии «Национальная лига за демократию» вместе с ее лидером Аунг Сан Су Чжи, которая убедительно выиграла выборы в ноябре 2020 года после серьезного поражения представителей вооруженных сил.

После переворота в стране, которая всего за несколько лет до этого сбежала из-под власти другого неудавшегося режима хунты, происходят массовые общественные протесты.

После переворота правительство несколько раз пыталось закрыть доступ в Интернет для всей страны, блокировало доступ к социальным сетям, чтобы помешать гражданам организовывать новые протесты, и в настоящее время пытается принять новый драконовский закон о безопасности, который позволил бы ему более легкий и беспрепятственный доступ к личным данным и истории просмотров любого пользователя». ***(Catalin Cimpanu. Malaysia arrests 11 suspects for hacking government sites // ZDNet (https://www.zdnet.com/article/malaysia-arrests-11-suspects-for-hacking-government-sites/). 19.02.2021).***

***

«Министерство юстиции США сегодня обнародовало новые обвинения против Lazarus Group - кодового названия, которое было присвоено спонсируемым государством военным хакерским группам Северной Кореи.

В новом обвинительном заключении расширяются обвинения, первоначально выдвинутые против Пак Джин Хёка, северокорейского военного хакера, обвиненного США в сентябре 2018 года в его причастности к взломам Sony, атакам вымогателя WannaCry и кибер-ограблениям банков.

В новом обвинительном заключении, опубликованном сегодня, обвиняются еще два северокорейских хакера, а именно Джон Чан Хёк (전 창혁), 31 год, и Ким Ир (), 27 лет, и расширяет обвинения, выдвинутые против Пака в 2018 году.

Официальные лица США заявляют, что эти три хакера являются частью подразделений Главного разведывательного управления (RGB), северокорейского военного разведывательного агентства, часть которого они участвовали во всемирной хакерской кампании, которая началась в 2014 году и включает в себя:

Взлом Sony Pictures Entertainment в 2014 году в отместку за то, что студия выпустила фильм «Интервью».

Кибер-ограбления в банках Вьетнама, Бангладеш, Тайваня, Мексики, Мальты и по всей Африке. Группа нацелена на систему денежных переводов SWIFT банка, пытаясь украсть более 1,2 миллиарда долларов.

Атаки с обналичиванием банкоматов с использованием вредоносного ПО FASTCash. Одна успешная такая атака произошла в октябре 2018 года, когда группа украла 6,1 миллиона долларов у пакистанского BankIslami.

Вспышка программы-вымогателя WannaCry в мае 2017 г.

Создание и распространение криптовалютных приложений с вредоносным ПО, которые крадут средства пользователей. Примеры включают Celas Trade Pro, WorldBit-Bot, iCryptoFx, Union Crypto Trader, Kupay Wallet, CoinGo Trade, Dorusio, CryptoNeuro Trader и Ants2Whale.

Взломы порталов обмена криптовалют. Министерство юстиции заявило, что RGB нацелился на сотни таких организаций и украл десятки миллионов долларов США.

Кампании целевого фишинга, нацеленные на оборонных подрядчиков США, энергетические компании, аэрокосмические компании, технологические компании, Государственный департамент США и Министерство обороны США.

Создание поддельной криптовалютной компании и выпуск токена Marine Chain Token. Министерство юстиции США заявило, что эта схема позволила бы пользователям приобретать в собственность морские суда с помощью токена криптовалюты, что позволило бы северокорейскому государству получить доступ к средствам инвесторов и обойти санкции США.

Официальные лица США заявили, что, хотя кампании были направлены на сбор разведданных, большинство из них были преступными попытками собрать средства для режима королевства отшельников.

Помощник генерального прокурора Джон Демерс назвал трех хакеров и Lazarus Group «ведущими грабителями банков в мире» и «преступным синдикатом с флагом».

ЕЩЕ ОДИН ДЕНЕЖНЫЙ МУЛ ЗАРЯЖЕН

Но сегодня Министерство юстиции также заявило, что предъявило обвинение гражданину Канады по имени Галеб Алаумари в том, что он помог Lazarus Group отмыть часть их украденных средств.

«Алаумари активно занимался отмыванием денег хакерами, задействованными в схемах обналичивания банкоматов, ограблениях банков с использованием киберпреступников, схемах компрометации деловой электронной почты (BEC) и других схемах онлайн-мошенничества», - заявили представители Министерства юстиции США.

Он якобы организовал бригады отмывателей денег в США и Канаде, чтобы получать украденные средства, а затем переводить их на другие счета, находящиеся под контролем хакеров.

Это включало отмывание средств, украденных в результате атаки по обналичиванию банкоматов BankIslami, еще одно снятие наличных через банкомат в индийском банке, которое произошло в 2018 году, и средства, украденные из мальтийского банка в 2019 году.

Алаумари теперь является третьим корейским банком Nortk, которому Nortk предъявлено обвинение в США после того, как Министерство юстиции предъявило обвинение двум гражданам Китая в марте 2020 года.

Копия сегодняшнего обвинительного заключения доступна здесь в формате PDF.

Помимо обвинений Министерства юстиции, Агентство кибербезопасности и безопасности инфраструктуры США также опубликовало сегодня отчет о вредоносном ПО AppleJeus, которое Lazarus Group часто использовала во время атак на порталы обмена криптовалютой». ***(Catalin Cimpanu. US charges two more members of the 'Lazarus' North Korean hacking group // ZDNet (https://www.zdnet.com/article/us-charges-two-more-members-of-the-lazarus-north-korean-hacking-group/). 17.02.2021).***

***

«Голландская полиция разместила «дружеские» сообщения на двух крупнейших сегодня хакерских форумах, предупреждая киберпреступников, что «размещение криминальной инфраструктуры в Нидерландах - безнадежное дело».

Сообщения были опубликованы после операции «Божья коровка», в ходе которой правоохранительные органы нескольких стран вмешались, чтобы остановить Emotet, один из крупнейших ботнетов на сегодняшний день.

Голландская полиция сыграла решающую роль в уничтожении Emotet после того, как ее сотрудники захватили два из трех ключевых серверов управления и контроля Emotet, которые находились в Нидерландах.

Но сегодня голландская полиция сообщила, что после уничтожения Emotet ее сотрудники также посетили Raid и XSS, два общедоступных и очень популярных хакерских форума, и разместили сообщения, чтобы отговорить других злоумышленников от злоупотреблений голландских хостинг-провайдеров для размещения бот-сетей или других формы киберпреступности.

Сообщение на английском языке было размещено на Raid, форуме, популярном среди торговцев украденными данными, а второе сообщение на русском языке было размещено на XSS (ранее известном как DamageLab), русскоязычном форуме, на котором хакеры арендуют доступ к вредоносному ПО. a-service и форум, который сегодня часто посещают ведущие банды вымогателей.

Сообщения, как видно выше, предупреждают хакеров, что «размещение криминальной инфраструктуры в Нидерландах - безнадежное дело» и что голландская полиция планирует и дальше захватывать их инфраструктуру.

Также была включена ссылка на видео на YouTube, видео, которое заканчивается сообщением голландской полиции, в котором говорится: «Все делают ошибки. Мы ждем ваших».

Агрессивные сообщения не являются неожиданностью, по крайней мере, для экспертов по кибербезопасности, большинство из которых хорошо осведомлены об агрессивной позиции голландской полиции.

За последние годы голландская полиция оказалась в центре многих уничтожений ботнетов, больших и малых. Они арестовали владельцев двух провайдеров веб-хостинга, которые обычно размещали DDoS-ботнеты, сняли 15 различных DDoS-ботнетов за неделю, перешли на перехват зашифрованных сообщений криптофона BlackBox, закрыли Ennetcom за обеспечение поддержки зашифрованного чата для групп киберпреступников и начали агрессивную охоту. фишеры, операторы вредоносных программ и пользователи сервисов DDoS-найма.

Голландская полиция также в настоящее время вместе с немецкой полицией находится в центре операции по массовому удалению вредоносного ПО Emotet с зараженных хостов». ***(Catalin Cimpanu. Dutch police post 'friendly' warnings on hacking forums // ZDNet (https://www.zdnet.com/article/dutch-police-post-friendly-warnings-on-hacking-forums/). 17.02.2021).***

***

Технічні аспекти кібербезпеки

Виявлені вразливості технічних засобів та програмного забезпечення

«Уязвимости в протоколах связи, используемых миллионами устройств Интернета вещей (IoT) и операционных технологий (OT), могут позволить кибератакам перехватывать данные и манипулировать ими.

Уязвимости в некоторых стеках TCP / IP подробно описаны исследователями кибербезопасности из Forescout, которые назвали набор из девяти новых уязвимостей «Number: Jack».

Он формирует текущее исследование, проводимое компанией по кибербезопасности в рамках проекта Memoria, инициативы по изучению уязвимостей в стеках TCP / IP и способов их устранения.

Последние раскрытия основаны на фундаментальном аспекте связи TCP во встроенных устройствах: генерации начального порядкового номера (ISN). Эти ISN предназначены для обеспечения уникальности каждого протокола TCP между двумя компьютерами или другими устройствами, подключенными к Интернету, и того, что третьи стороны не могут вмешиваться или манипулировать соединениями.

Чтобы гарантировать это, ISN должны генерироваться случайным образом, чтобы злоумышленник не мог его угадать, перехватить или подделать. Это основа компьютерной безопасности, которая была известна еще в 90-х годах, но когда дело доходит до безопасности устройств Интернета вещей, исследователи обнаружили, что эта старая уязвимость присутствовала, поскольку числа не были полностью случайными, поэтому структура номеров ISN в этих TCP-коммуникациях можно было предсказать.

«Это в основном исправлено в Windows и Linux, а также в типичном мире ИТ. Но когда вы смотрите на мир Интернета вещей, это происходит снова», - сказал ZDNet Даниэль душ Сантуш, менеджер по исследованиям Forescout.

«Нам или злоумышленнику нетрудно найти этот тип уязвимости, потому что вы можете ясно увидеть, как числа, генерируемые стеком, предсказуемы», - добавил он.

Предсказывая существующее TCP-соединение, злоумышленники могут закрыть его, по сути вызывая атаку типа «отказ в обслуживании», предотвращая передачу данных между устройствами. В качестве альтернативы они могут захватить его и ввести свои собственные данные в сеанс, с помощью которых можно перехватить незашифрованный трафик, добавить загрузку файлов для обслуживания вредоносных программ или использовать HTTP-ответы, чтобы направить жертву на вредоносный веб-сайт. Злоумышленники также могут злоупотреблять TCP-соединениями встроенных устройств для обхода протоколов аутентификации, которые потенциально предоставляют злоумышленникам дополнительный доступ к сетям.

Все уязвимости были обнаружены и раскрыты соответствующим поставщикам и специалистам по обслуживанию затронутых стеков TCP / IP к октябрю 2020 года.

Стеки TCP / IP, содержащие уязвимости, включают несколько стеков с открытым исходным кодом, проанализированных в предыдущем исследовании Forescout, включая uIP, FNET, picoTCP, Nut / Net, cycloneTCP и uC / TCP-IP. Уязвимости также были обнаружены в Nucleus NET от Siemens, NDKTCPIP от Texas Instruments и MPLAB Net от Microchip.

Большинство поставщиков установили исправления для защиты устройств от уязвимостей или находятся в процессе этого, хотя исследователи отмечают, что никто не отреагировал на раскрытие информации. ZDNet попытался связаться с каждым из поставщиков, подробно описанных в исследовательском документе, для получения ответа.

Forescout публично не определила точные устройства, которые полагаются на девять стеков, которые, как было обнаружено, имеют уязвимости, чтобы предотвратить их превращение в потенциальные жертвы атак. Однако они

отмечают, что все системы, включая медицинские устройства, системы мониторинга ветряных турбин и системы хранения, зависят от систем, которые, как известно, используют проверенные стеки.

Чтобы защитить себя от атак, Forescout Research Labs выпустила скрипт с открытым исходным кодом, который помогает идентифицировать стеки, в которых обнаружены уязвимости в рамках проекта Memoria.

Если в сети обнаружены эти уязвимости, рекомендуется применить исправления безопасности, чтобы злоумышленники не могли воспользоваться ими. Также предполагается, что, когда невозможно исправить устройства IoT или OT, затронутые продукты сегментируются в часть сети, что снижает вероятность взлома.

Исследование также служит напоминанием о том, что, когда речь идет о безопасности устройств IoT, необходимо извлечь уроки безопасности из ИТ-безопасности, которые необходимо применять, особенно когда речь идет об основах, о которых известно уже несколько десятилетий.

«Основы Интернета вещей уязвимы не только для одного поставщика или конкретного устройства - это касается нескольких типов устройств и программных компонентов, используемых в этих устройствах. Часто они имеют схожие типы уязвимостей», - сказал душ Сантуш.

«Причина, по которой мы просмотрели стеки TCP, состоит в том, чтобы показать, что история снова повторяется в нескольких стеках. Это доказывает, что люди должны смотреть на то, что происходило раньше, и как это влияет на их операции - на всем протяжении цепочки поставок IoT», - сказал он». ***(Danny Palmer. This old security vulnerability left millions of Internet of Things devices vulnerable to attacks // ZDNet (https://www.zdnet.com/article/this-old-security-vulnerability-left-millions-of-internet-of-things-devices-vulnerable-to-attacks/). 10.02.2021).***

***

«Сегодня Google заявила, что выплатила более 6,7 миллиона долларов в виде вознаграждения за обнаружение ошибок 662 исследователям безопасности из 62 стран за отправку отчетов об уязвимостях в продуктах Google в прошлом году.

Это самый крупный призовой фонд, выплаченный исследователям в области безопасности на сегодняшний день, по сравнению с 6,5 млн долларов, которые компания выплатила в 2019 году.

Большая часть прошлогодних призов за ошибки была присуждена в рамках Chrome VRP (Программа вознаграждений за уязвимости), в рамках которой исследователям безопасности было выделено более 2,1 миллиона долларов за 300 ошибок, обнаруженных во флагманском браузере Google.

Еще одной важной VRP были программы компании для Android. Google заявила, что выделила 1,74 миллиона долларов за ошибки, обнаруженные в коде ОС Android, и еще 270 000 долларов в VRP Google Play за ошибки, обнаруженные в самых популярных и широко используемых приложениях Android из Play Store.

Среди основных достижений Android VRP в прошлом году Google перечислил следующее:

Мы наградили наш первый бонус за предварительную версию Android 11 для разработчиков, который составил более 50 000 долларов по 11 отчетам. Это позволило нам заблаговременно исправить проблемы до официального выпуска Android 11.

Гуан Гун (@oldfresher) и его команда из 360 Alpha Lab, Qihoo 360 Technology Co. Ltd., теперь удерживают рекордные восемь эксплойтов (30% от общего количества) в таблице лидеров. Совсем недавно Alpha Lab представила впечатляющий эксплойт удаленного root-доступа в один клик, нацеленный на последние устройства Android. Они сохраняют максимальную выплату Android (161 337 долларов плюс еще 40 000 долларов от Chrome VRP) за свой эксплойт 2019 года.

Другой исследователь представил еще два эксплойта и борется за первое место в истории с внушительными выплатами за все время эксплойтов в размере 400000 долларов.

Мы запустили ряд пилотных программ вознаграждения, чтобы направить исследователей безопасности в дополнительные области интересов, включая ОС Android Auto, написание фаззеров для кода Android и программу вознаграждений для наборов микросхем Android.

Вдобавок к этому, Google также сообщил, что более 400 000 долларов было отправлено исследователям безопасности в рамках программы исследовательских грантов, которую компания использует для финансирования инновационных областей исследований в области безопасности.

В прошлом году гранты получили более 180 исследователей в области безопасности, которые прислали обратно 200 отчетов об ошибках, которые выявили 100 подтвержденных уязвимостей в продуктах Google и экосистеме с открытым исходным кодом.

В этом году Google VRP исполняется 10 лет». ***(Catalin Cimpanu. Google paid $6.7 million to bug bounty hunters in 2020 // ZDNet (https://www.zdnet.com/article/google-paid-6-7-million-to-bug-bounty-hunters-in-2020/). 04.02.2021).***

***

«Сервисы DDoS по найму нашли способ злоупотреблять серверами Plex Media для отражения нежелательного трафика и усиления распределенных атак типа «отказ в обслуживании» (DDoS), сообщила в среду охранная компания Netscout.

Предупреждение компании предупреждает владельцев устройств, которые поставляются с Plex Media Server, веб-приложением для Windows, Mac и Linux, которое обычно используется для потоковой передачи видео или аудио и управления мультимедийными активами.

Приложение может быть установлено на обычных веб-серверах или обычно поставляется с сетевыми хранилищами (NAS), цифровыми медиаплеерами или другими типами устройств IoT для потоковой передачи мультимедиа.

СЕРВЕРЫ PLEX MEDIA ПРОБИВАЮТ ДЫРУ В NAT МАРШРУТИЗАТОРА

Netscout сообщает, что когда сервер / устройство, на котором запущено приложение Plex Media Server, загружается и подключается к сети, он запускает локальное сканирование для других совместимых устройств через протокол обнаружения простых служб (SSDP).

Проблема возникает, когда Plex Media Server обнаруживает локальный маршрутизатор с включенной поддержкой SSDP. Когда это произойдет, Plex Media Server добавит правило переадресации NAT к маршрутизатору, предоставляя свою службу Plex Media SSDP (PMSSDP) непосредственно в Интернете через порт UDP 32414.

Поскольку протокол SSDP был известен в течение многих лет как идеальный вектор для увеличения масштабов DDoS-атаки, это делает серверы Plex Media интересным и неиспользованным источником DDoS-ботов для операций DDoS-по найму.

Netscout утверждает, что злоумышленникам нужно только сканировать Интернет на предмет устройств с включенным этим портом, а затем злоупотреблять ими, чтобы усилить веб-трафик, который они отправляют жертве DDoS-атаки.

Согласно Netscout, коэффициент усиления составляет около 4,68, при этом сервер Plex Media усиливает входящие пакеты PMSSDP с 52 байтов до примерно 281 байта перед отправкой пакета жертве.

27K + СЕРВЕРОВ PLEX MEDIA ДОСТУПНЫ В ИНТЕРНЕТЕ

Фирма по безопасности заявила, что просканировала Интернет и обнаружила 27000 серверов Plex Media, оставшихся открытыми в сети, которые могут быть использованы для DDoS-атак.

Более того, некоторые серверы уже подверглись злоупотреблениям. Netscout заявил, что не только видел DDoS-атаки с использованием серверов Plex Media, но и что этот вектор теперь становится обычным явлением.

«Как это обычно бывает с новыми векторами DDoS-атак, похоже, что после начального периода использования опытными злоумышленниками с доступом к индивидуализированной инфраструктуре DDoS-атак, PMSSDP был превращен в оружие и добавлен в арсеналы так называемых Booter / Stresser DDoS- услуги по найму, что делает его доступным для большинства злоумышленников», - заявили в компании.

Согласно Netscout, прошлые атаки PMSSDP достигли примерно 2-3 Гбит / с, но серверы могут быть объединены с другими векторами для гораздо более крупных атак.

Это второе предупреждение Netscout о том, что в этом году в дикой природе был обнаружен новый вектор атаки DDoS. В январе компания предупредила, что серверы протокола удаленного рабочего стола Windows (RDP) также использовались для DDoS-атак.

Представитель Plex сообщил сегодня ZDNet, что компания в настоящее время работает над патчем, который «добавляет дополнительный уровень защиты для тех серверов, которые могли быть случайно обнаружены», который компания

планирует выпустить в ближайшее время». ***(Catalin Cimpanu. Plex Media servers are being abused for DDoS attacks // ZDNet (https://www.zdnet.com/article/plex-media-servers-are-being-abused-for-ddos-attacks/). 05.02.2021).***

***

«В то время как индустрия информационной безопасности привыкла читать (и выкачивать) FUD об уязвимостях программного обеспечения, привлекающие внимание исследования показывают, что в 2019 году было использовано около 500 уязвимостей - несмотря на создание 18000 новых CVE.

Kenna Security, американская компания, занимающаяся информационной безопасностью, считает, что, несмотря на то, что тысячам уязвимостей в течение года был присвоен номер отслеживания Common Vulnerabilities and Exploitations (CVE), только 473 из них активно эксплуатировались способами, которые могли нанести ущерб предприятиям.

Это составляет всего 2,6 процента уязвимостей, зарегистрированных в течение года, что проливает новый свет на масштаб угрозы для предприятий, подключенных к Интернету.

Соучредитель и технический директор Кенны Эд Беллис сказал The Register, что анализ, проведенный его фирмой, был сосредоточен на тех CVE, которые могут повлиять на ее клиентов. По его словам, даже эту цифру в 473 человека можно уменьшить. Хотя компания не отфильтровала цифру в 18 000 CVE, например, чтобы посмотреть только на те, которые влияют на корпоративное программное обеспечение, разница между ними разительна.

«Всего лишь 6 процентов из этих 473 уязвимостей когда-либо широко использовались более чем 1/100 организаций», - говорится в отчете Kenna Security. «Тот факт, что эксплойт существует «в дикой природе», не означает, что он бушует в Интернете».

В отчете говорится: «К моменту публикации в списке CVE код эксплойта уже был доступен для> 50% уязвимостей (в конечном итоге использовавшихся в реальных условиях). К счастью для защитников, выпуск исправлений совпадает с публикацией более 80% из них. CVE».

Уязвимости существуют, но популярное мнение о том, что все ужасно небезопасно, а иногда только чистая удача спасает нас от кражи данных, атак типа «отказ в обслуживании» и многого другого, может оказаться неверным. Представьте себе это!

CVE, CNA, CVSS - можете ли вы использовать еще одну аббревиатуру?

CVE, хотя и несовершенные, являются широко принятой мерой количества и серьезности уязвимостей в открытом доступе. Дэн Меллингер из Kenna Security добавил, что за последние несколько лет было создано большое количество органов нумерации CVE (CNA), что способствовало росту зарегистрированных CVE. В настоящее время существует более 150 организаций, которые имеют право назначать CVE, хотя большинство из них являются поставщиками, которые берут на себя ответственность только за свои собственные продукты (например, в Великобритании в настоящее время всего три CNA: Canonical, Snyk и Sophos, все из которых попадают в эту скобку).

Ученые также подвергли сомнению повторяемость и последовательность оценки CVE, поскольку в немецком университете в настоящее время выполняется исследовательский проект по Системе оценки общих уязвимостей, в котором основное внимание уделяется тому, почему и как разные люди выставляют оценки, которые дают очень разные результаты.

Кроме того, причины CVE различаются. В то время как большинство FUD вокруг приливных волн уязвимостей, подавляющих информационные блоки, вызывают в воображении образ групп злонамеренных людей, безжалостно выявляющих и использующих уязвимости для совершения новых злодеяний, правда иногда оказывается более прозаической, чем это.

Google проиллюстрировал этот очень человеческий провал ранее в этом месяце, когда его Project Zero издал старый добрый стон по поводу дерьмовых исправлений безопасности, неспособных полностью исправить проблемы с уведомлением CVE. Двумя днями позже Google Chromium продемонстрировал, на что жаловался Project Zero, с помощью старого Chromium нулевого дня, который он не смог должным образом исправить в ноябре». ***(Gareth Corfield. Just 2.6% of 2019's 18,000 tracked vulnerabilities were actively exploited in the wild // The Register (https://www.theregister.com/2021/02/18/cve_exploitation_2_6pc_kenna_security/). 18.02.2021).***

***

«QNAP устранил критическую уязвимость системы безопасности в приложен ии Surveillance Station, которая позволяет злоумышленникам удаленно выполнять вредоносный код на устройствах сетевого хранения (NAS), на которых запущено уязвимое программное обеспечение.

Surveillance Station - это система управления видео (VMS) сетевого наблюдения QNAP, программное решение, которое может помочь пользователям управлять и контролировать до 12 IP-камер.

Это стандартное приложение Turbo NAS с поддержкой более 3000 моделей IP-камер, которое можно установить из центра приложений QTS компании.

В последних версиях приложения исправлена критическая ошибка RCE

Критический недостаток безопасности, исправленный сегодня QNAP, - это уязвимость, связанная с переполнением буфера в стеке, которая влияет на устройства QNAP NAS, на которых работает Surveillance Station.

«В случае эксплуатации эта уязвимость позволяет злоумышленникам выполнять произвольный код», - поясняет QNAP в сегодняшнем сообщении по безопасности.

При успешном использовании его для выполнения произвольного кода злоумышленники также будут регулярно подрывать любые службы безопасности или антивирусные решения, работающие на скомпрометированном устройстве.

QNAP уже устранила критическую уязвимость в следующих версиях программного обеспечения:

Surveillance Station 5.1.5.4.3 (и выше) для NAS с процессором ARM (64-разрядная ОС) и NAS с процессором x86 (64-разрядная ОС)

Surveillance Station 5.1.5.3.3 (и выше) для NAS с процессором ARM (32-разрядная ОС) и NAS с процессором x86 (32-разрядная ОС)

Компания также исправила уязвимость межсайтового скриптинга (XSS) средней степени серьезности, которая затрагивала более ранние версии приложения Photo Station, которое использовалось для загрузки изображений на устройство QNAP NAS, создания альбомов или удаленного просмотра их.

«В случае эксплуатации эта уязвимость позволяет удаленным злоумышленникам внедрить вредоносный код», - утверждает QNAP. Ошибка безопасности устранена в Photo Station 6.0.11 и более поздних версиях.

Как обновиться до последних версий

Учитывая рейтинги серьезности уязвимостей, клиенты должны как можно скорее обновить оба приложения до последних доступных версий…». ***(Sergiu Gatlan. QNAP patches critical vulnerability in Surveillance Station NAS app // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/qnap-patches-critical-vulnerability-in-surveillance-station-nas-app/). 17.02.2021).***

***

«Microsoft исправила уязвимость повышения привилегий в антивирусе Microsoft Defender (ранее - Защитник Windows), которая могла позволить злоумышленникам получить права администратора в незащищенных системах Windows.

Согласно статистике Microsoft, антивирус Microsoft Defender Antivirus - это решение по умолчанию для защиты от вредоносных программ в более чем 1 миллиардах систем под управлением Windows 10.

CVE-2021-24092 влияет на версии Защитника, начиная с 2009 года, и влияет на клиентские и серверные версии, начиная с Windows 7 и выше.

Злоумышленники с базовыми правами пользователя могут использовать его локально в рамках атак низкой сложности, которые не требуют взаимодействия с пользователем.

Уязвимость также влияет на другие продукты безопасности Microsoft, включая, помимо прочего, Microsoft Endpoint Protection, Microsoft Security Essentials и Microsoft System Center Endpoint Protection.

SentinelOne обнаружил уязвимость и сообщил об этой уязвимости в ноябре 2020 года. Во вторник Microsoft выпустила патч вместе с другими обновлениями безопасности, опубликованными в рамках февральского патча 2021 года во вторник.

Не обнаруживается более десяти лет

Уязвимость была обнаружена в драйвере BTR.sys (также известном как средство удаления времени загрузки), используемом в процессе исправления для удаления файлов и записей реестра, созданных вредоносным ПО в зараженных системах.

«До исправления уязвимость оставалась неоткрытой в течение 12 лет, вероятно, из-за характера активации этого конкретного механизма», - говорится в отчете SentinelOne, опубликованном сегодня и заранее переданном BleepingComputer.

«Мы предполагаем, что эта уязвимость оставалась не обнаруженной до сих пор, потому что драйвер обычно не присутствует на жестком диске, а скорее сбрасывается и активируется при необходимости (со случайным именем), а затем удаляется».

Последней версией Microsoft Malware Protection Engine, подверженной этой уязвимости, является версия 1.1.17700.4. Первая версия, в которой была исправлена ошибка, - 1.1.17800.5.

Системы, исправленные для защиты от этой уязвимости, должны работать под управлением Microsoft Malware Protection Engine версии 1.1.17800.5 или более поздней.

Дополнительная информация о том, как проверить версию модуля защиты от вредоносных программ в вашей системе, доступна здесь.

Обновление безопасности Защитника устанавливается автоматически

Редмонд говорит, что обновление безопасности CVE-2021-1647 будет автоматически установлено в системах, на которых работают уязвимые версии Microsoft Defender, если автоматические обновления включены.

Microsoft Defender автоматически обновляет как модуль защиты от вредоносных программ (компонент, используемый для сканирования, обнаружения и очистки), так и определения вредоносных программ на корпоративных и домашних устройствах.

Хотя Microsoft Defender может проверять наличие обновлений ядра и определений несколько раз в день, клиентам рекомендуется вручную проверять наличие обновлений, если они хотят немедленно установить обновления безопасности.

«Конечно, хотя кажется, что уязвимость не использовалась, злоумышленники, вероятно, придумают, как использовать ее в незащищенных системах», - заключил SentinelOne.

«Кроме того, поскольку уязвимость присутствует во всех версиях Защитника Windows, начиная примерно с 2009 года, вполне вероятно, что многие пользователи не смогут применить исправление, что сделает их уязвимыми для будущих атак»…». ***(Sergiu Gatlan. 12-year-old Windows Defender bug gives hackers admin rights // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/12-year-old-windows-defender-bug-gives-hackers-admin-rights/). 11.02.2021).***

***

«Как обнаружил Wordfence, критические уязвимости высокой степени серьезности в плагине Responsive Menu WordPress сделали более 100 000 сайтов уязвимыми для атак.

Responsive Menu - это плагин WordPress, разработанный, чтобы помочь администраторам создавать ответственные меню сайтов, совместимые с W3C и готовые для мобильных устройств.

Недостатки исправлены в прошлом месяце

В целом команда Wordfence Threat Intelligence обнаружила три уязвимости, которые могут быть использованы злоумышленниками с базовыми правами

пользователя на загрузку произвольных файлов и удаленное выполнение произвольного кода.

Первый недостаток позволяет проверенным злоумышленникам загружать произвольные файлы, что в конечном итоге позволяет им выполнять удаленное выполнение кода.

Две другие уязвимости позволяют потенциальному злоумышленнику подделывать запросы на изменение настроек плагина, что, в свою очередь, позволяет им загружать произвольные файлы, позволяя удаленно выполнять код.

Чтобы воспользоваться критической уязвимостью, злоумышленники, вошедшие в систему как подписчики или другой низкоуровневый пользователь, должны загрузить темы меню, заархивированные в виде файлов ZIP и содержащие вредоносные файлы PHP.

После извлечения архива для установки злоумышленник может получить доступ к файлам через интерфейс сайта для удаленного выполнения вредоносного кода, что в конечном итоге может привести к полному захвату сайта.

ExpressTech, компания, стоящая за Responsive Menu, исправила проблемы безопасности 19 января 2021 года после нескольких попыток контакта в период с 17 декабря по 4 января.

В конце концов, ответы на запросы отчета были даны 10 января, после того, как Wordfence был передан команде WordPress Plugins.

Поскольку проблемы с безопасностью затрагивают версии Responsive Menu с 4.0.0 до 4.0.3 (или работающие в устаревшем режиме), пользователям рекомендуется немедленно выполнить обновление до версии 4.0.4, которая устраняет ошибки и предотвращает попытки эксплуатации.

«Все три уязвимости могут привести к захвату сайта, что может иметь последствия, включая бэкдоры, спам-инъекции, вредоносные перенаправления и другие вредоносные действия», - добавил Wordfence.

Примерно 50 000 сайтов все еще подвержены атакам

Несмотря на то, что патченная версия Responsive Menu 4.0.4 была выпущена 19 января, до вчерашнего дня было зарегистрировано чуть более 50 000 новых загрузок на основе статистики, доступной в репозитории плагина WordPress.

Поскольку эти цифры включают как обновления, так и новые установки, почти 50 000 сайтов WordPress, использующих Адаптивное меню, все еще могут быть взломаны злоумышленниками.

Ранее на этой неделе Wordfence также сообщил о двух критических CSRF-уязвимостях высокой степени серьезности в плагине NextGen Gallery, которые позволяют хакерам внедрять бэкдоры, создавать мошеннических администраторов и потенциально захватить более 530 000 сайтов WordPress, на которых все еще используются не исправленные версии плагинов.

WordPress должен устанавливать обновления безопасности плагинов как можно скорее после их выпуска разработчиками, поскольку злоумышленники часто используют уже исправленные уязвимости в устаревших плагинах WordPress в своих атаках». ***(Sergiu Gatlan. Buggy WordPress plugin exposes 100K sites to takeover attacks // Bleeping Computer®***

(https://www.bleepingcomputer.com/news/security/buggy-wordpress-plugin-exposes-100k-sites-to-takeover-attacks/). 11.02.2021).

***

«Singtel и Медицинский исследовательский институт QIMR Berghofer - последние компании, которые раскрыли утечки данных, вызванные уязвимостью в программном обеспечении безопасной передачи файлов Accellion FTA.

Accellion - разработчик продуктов для безопасной передачи файлов, которые позволяют организациям передавать конфиденциальные файлы людям за пределами своей организации.

В середине декабря Accellion объявил, что им стало известно об активно эксплуатируемой уязвимости нулевого дня в их продукте для безопасной передачи файлов FTA, которая позволяла злоумышленникам получать доступ к данным клиентов.

Хотя они выпустили патч на Рождество, как только узнали об уязвимости, к тому времени, когда некоторые компании смогли исправить это, злоумышленники уже получили доступ к своим данным.

Поскольку сервис Accellion FTA используется многочисленными правительственными учреждениями, образовательными учреждениями и компаниями, мы начали видеть широкомасштабное воздействие, поскольку компании сообщают о связанных утечках данных.

Предыдущие нарушения данных включают Резервный банк Новой Зеландии, Австралийскую комиссию по ценным бумагам и инвестициям (ASIC) и Управление аудитора штата Вашингтон («SAO»)…». ***(Lawrence Abrams. Singtel, QIMR Berghofer report Accellion-related data breaches // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/singtel-qimr-berghofer-report-accellion-related-data-breaches/). 11.02.2021).***

***

«На этой неделе в репозиторий с открытым исходным кодом npm было опубликовано более 275 новых пакетов, названных в честь частных компонентов, используемых внутри крупных компаний.

Эти пакеты npm идентичны пакетам для проверки концепции, созданным Алексом Бирсаном, исследователем, которому недавно удалось проникнуть в основные 35 технологических компаний и получить более шестизначные суммы вознаграждений за ошибки.

В течение 48 часов после обнародования информации о Бирсане, актеры-подражатели начали отправлять аналогичные пакеты в npm, вероятно, в стремлении заработать вознаграждение за ошибки.

Бирсан подтвердил BleepingComputer, что он не стоит за этими имитационными пакетами и что это разные актеры, идущие по его стопам.

Исследователь взломал 35 технологических компаний в ходе новой атаки на цепочку поставок

Недавно BleepingComputer впервые сообщил об атаке на цепочку поставок, которая поразила более 35 технологических компаний, в том числе Microsoft, Apple, PayPal, Tesla, Uber, Yelp, Shopify и других.

Исследователь, Алекс Бирсан, воспользовался внутренним недостатком дизайна инструментов разработки с открытым исходным кодом, который называется «путаница в зависимостях» или «путаница в пространстве имен», чтобы присвоить имена частных зависимостей, используемых крупными компаниями в общедоступных репозиториях с открытым исходным кодом, включая npm, PyPI. и RubyGems.

Сегодня отчет Sonatype показывает, что другие участники подражания теперь имитируют исследования Бирсана, наводняя репозиторий npm пакетами-подражателями, помеченными «только для целей исследования безопасности».

Актеры-подражатели наводняют npm идентичными пакетами

В течение последних 48 часов группа Sonatype Security Research, частью которой я являюсь, заметила внезапный всплеск количества подозрительных пакетов, обнаруженных нашими автоматизированными системами обнаружения вредоносных программ, и начала анализировать эти пакеты.

И тогда это имело смысл. Подавляющее большинство из 275+ компонентов, которые были отмечены и продолжают поступать на момент написания, являются двойниками пакетов PoC Бирсана, которые позволили ему взломать более 35 технологических компаний в рамках его этического исследования.

Но Бирсан говорит BleepingComputer, что он не стоит за этими подражателями «исследовательских» пакетов, хотя он признался, что загрузил еще несколько пакетов сегодня под своей реальной учетной записью npm.

«Сегодня я загрузил еще несколько пакетов».

«Мои тесты всегда будут собирать одни и те же неконфиденциальные данные и будут загружены из моей учетной записи с моей контактной информацией в самом коде».

«Однако вполне естественно ожидать, что другие охотники за ошибками или даже злоумышленники тоже начнут загружать пакеты сейчас, и я не могу контролировать, что они делают», - сказал Бирсан в заявлении BleepingComputer.

Исследователь подозревает, что люди гонятся за наградой и поэтому идут по его стопам.

Одним из таких примеров может быть пакет npm «shopify-cloud», названный в честь RubyGem с тем же именем, которое Бирсан использовал для выполнения своего PoC-кода из систем Shopify через путаницу зависимостей.

Хотя пакет npm называется «shopify-cloud», маловероятно, что он повлияет на систему сборки Shopify, которая использовала пакет RubyGem (не npm) с этим именем, если они также не используют частную зависимость npm под названием «shopify- облако."

Другие пакеты-подражатели называются «apple-cloud», «aol-slideshow» и, конечно же, «dependency-confusion-poc2», причем последний из них чрезмерно честен.

Код для «aol-slideshow» делает DNS-вызов на сервер автора и передает основную информацию, такую как IP-адрес, имя пользователя компьютера и

текущий каталог, выполняя «обратный вызов», который уведомит издателя пакета об успешной атаке.

Перед попыткой кражи код сначала пытается подключиться к DNS-серверам, контролируемым автором, в этом примере *.v1.ldd.pw

В случае сбоя соединения или установления слишком долгого времени код незаметно устанавливает DNS-серверы на серверы Google (8.8.8.8 и 8.8.4.4), чтобы не вызывать никаких подозрений, связанных с тайм-аутами.

В другом PoC-пакете под названием "Spectrum-css-temp", который видел BleepingComputer, автор, похоже, внес небольшую вариацию в название пакета Adobe Spectrum CSS.

Тем не менее, скваттер забыл удалить исходную контактную информацию Бирсана из комментариев к коду, как это было видно BleepingComputer.

Но нельзя достоверно проверить, действительно ли имена этих пакетов противоречат каким-либо именам частных зависимостей, используемым Apple, AOL и другими компаниями, или если эти частные зависимости существуют даже в каких-либо корпоративных системах.

В ходе нашего исследования Sonatype также обнаружила пакеты npm, которые отображают предупреждающее сообщение для разработчика, создающего внутренний проект, о том, что они должны использовать «частный реестр» для этого конкретного npm.

Неизвестно, был ли этот файл создан компанией, намеренно опечатавшей npm, или белой шляпой, пытающейся предупредить разработчиков.

Тем не менее, реестр npm, засыпанный этими пакетами-подражателями, обнаруженными Sonatype, является ярким признаком того, что путаница с зависимостями - проблема, которую нелегко решить, если репозитории с открытым исходным кодом не усиливают проверки того, кто может публиковать в этих репозиториях.

Что еще более важно, ответственность ложится на репозитории, чтобы предотвратить незаконное присвоение злоумышленниками имен частных компонентов / пространств имен, которые активно используются законными брендами.

В последнее время npm неоднократно подвергался атакам вредоносных пакетов с типосквотированием.

Ранее в этом месяце, НПМ снес три вредоносных пакетов, jquerry, и HTTP-прокси-middelware, которые были Ошибочное версии популярных законных пакетов, и третий имени меня.

Проблема путаницы в зависимостях, которую нелегко решить, теперь открывает возможность еще более сложных атак со стороны злоумышленников.

Бирсан считает, что эти атаки останутся, и что еще предстоит выяснить.

По-прежнему существует возможность повторного появления и роста таких атак, особенно на платформах с открытым исходным кодом, где нет простого решения для путаницы с зависимостями.

«В частности, я считаю, что поиск новых и умных способов утечки внутренних имен пакетов раскроет еще более уязвимые системы, а изучение альтернативных языков программирования и репозиториев для нацеливания

откроет некоторую дополнительную поверхность атаки для ошибок путаницы в зависимостях», - заключил исследователь ранее. в его сообщении в блоге.

По крайней мере, компаниям следует подумать о том, чтобы сквотировать свои собственные частные имена зависимостей в публичных репозиториях, включая их версии с опечатками (с ошибками).

Кроме того, следует оценить конфигурацию ваших инструментов разработки, чтобы убедиться, что как частные, так и общедоступные зависимости не будут случайно извлечены из общедоступного репозитория по умолчанию.

GitHub, компания, стоящая за npm, поделилась дополнительными советами по защите от атак путаницы зависимостей в своем блоге». ***(Ax Sharma. Copycats imitate novel supply chain attack that hit tech giants // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/copycats-imitate-novel-supply-chain-attack-that-hit-tech-giants/). 12.02.2021).***

***

«Telegram исправил проблему безопасности, из-за которой самоуничтожающиеся аудио- и видеофайлы не удалялись с устройств MacOS пользователя, как ожидалось.

Telegram предлагает режим секретного чата, который обеспечивает большую конфиденциальность, чем стандартные чаты.

В секретном чате все соединения зашифрованы, вы не можете пересылать сообщения другим пользователям, а все сообщения и мультимедиа можно настроить на автоматическое самоуничтожение и удаление со всех устройств по истечении определенного времени.

Вчера исследователь безопасности Дхирадж Мишра сообщил BleepingComputer, что обнаружил уязвимость в функции секретного чата в Telegram 7.3, в которой самоуничтожающийся носитель не удаляется с устройств получателей.

Выполняя аудит безопасности Telegram на macOS, Мишра обнаружил, что стандартные чаты могут пропускать путь песочницы, где хранятся полученные видео и аудио файлы.

Хотя этот путь не будет пропущен в секретных чатах, полученные медиафайлы все равно будут храниться в той же папке.

"В моем случае путь был (/ var / folder / x7 / khjtxvbn0lzgjyy9xzc18z100000gn / T /). При выполнении той же задачи в режиме секретного чата URI MediaResourceData (path: //) не просочился, но записанное аудио / видео сообщение все еще хранится по указанному выше пути», - пояснил Мишра в отчете об уязвимости.

Дишра обнаружил, что когда носитель самоуничтожился и был удален из чата, фактические медиафайлы все еще были доступны в папке компьютера.

«Боб (злоумышленник, использующий tdesktop macOS) и Алиса (жертва) общаются в режиме секретного чата, и Алиса отправляет записанное аудио / видео сообщение Бобу с таймером самоуничтожения на 20 секунд».

«Однако записанное сообщение удаляется из чата через 20 секунд, но по-прежнему остается в пользовательском пути Боба, здесь Telegram не может

предотвратить конфиденциальность для Алисы. В общем, функция самоуничтожения и не оставления следов не работает», - объясняет Мишра в сценарий атаки совместно с BleepingComputer.

Эта ошибка особенно касается пользователей, которые могут отправлять очень конфиденциальные видео другим пользователям Telgrams, ожидая, что приложение автоматически удалит их по истечении установленного времени…

Пароль сохранен в виде обычного текста

Помимо проблемы с безопасностью секретного чата, Мишра обнаружил, что Telegram хранил локальные коды доступа пользователя для разблокировки приложения в виде обычного текста на устройстве.

Эти пароли в виде открытого текста были сохранены в папке Users / [имя пользователя] / Library / Group Containers / 6N38VWS5BX.ru.keepcoder.Telegram / accounts-metadata в виде файла JSON.

Дишра сообщил об обеих уязвимостях 26 декабря 2020 года, и теперь они исправлены в Telegram 7.4.

За сообщение об обеих ошибках Мишра получил вознаграждение в размере 3000 долларов от Telegram». ***(Lawrence Abrams. Telegram privacy feature failed to delete self-destructing video files // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/telegram-privacy-feature-failed-to-delete-self-destructing-video-files/). 12.02.2021).***

***

«Adobe выпустила обновления безопасности, которые устраняют активно используемую уязвимость в Adobe Reader и другие критические ошибки в Adobe Acrobat, Magento, Photoshop, Animate, Illustrator и Dreamweaver.

В общей сложности компания устранила пятьдесят уязвимостей системы безопасности, затронувших семь продуктов, многие из которых были признаны критическими, поскольку допускают локальное выполнение произвольного кода.

Ошибка Adobe Reader, которая, как известно, активно используется в дикой природе, отслеживается как CVE-2021-21017. Эта уязвимость представляет собой ошибку переполнения буфера, которая позволяет вредоносному веб-сайту выполнять удаленное выполнение кода на уязвимом компьютере.

Ошибки выполнения кода являются наиболее серьезными, поскольку они могут позволить злоумышленникам выполнить практически любую команду в Windows, включая установку вредоносного ПО или захват компьютера.

Помимо активно используемой уязвимости Reader, Adobe также исправила другие критические уязвимости в своих продуктах, в том числе:

18 уязвимостей Magento

23 Уязвимости в Acrobat и Reader.

5 уязвимостей Photoshop

1 уязвимость Adobe Animate

2 уязвимости Adobe Illustrator

1 уязвимость Adobe Dreamweaver

Adobe рекомендует клиентам, использующим уязвимые продукты, как можно скорее обновить их до последних версий, чтобы заблокировать атаки, которые могут привести к успешной эксплуатации незащищенных установок…». ***(Lawrence Abrams. Adobe fixes critical Reader vulnerability exploited in the wild // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/adobe-fixes-critical-reader-vulnerability-exploited-in-the-wild/). 09.02.2021).***

***

«Исследователю удалось взломать внутренние системы более 35 крупных компаний, включая Microsoft, Apple, PayPal, Shopify, Netflix, Yelp, Tesla и Uber, в ходе новой атаки на цепочку поставок программного обеспечения.

Атака заключалась в загрузке вредоносного ПО в репозитории с открытым исходным кодом, включая PyPI, npm и RubyGems, которые затем автоматически распределялись по внутренним приложениям компании.

Традиционные атаки с типосквоттингом, основанные на тактике социальной инженерии или неправильном написании жертвой имени пакета, эта конкретная атака цепочки поставок является более сложной, поскольку она не требует никаких действий со стороны жертвы, которая автоматически получила вредоносные пакеты.

Это связано с тем, что атака использовала уникальный конструктивный недостаток экосистем с открытым исходным кодом, называемый путаницей зависимостей.

За свои этические исследования исследователь заработал более 130 000 долларов в виде вознаграждений за ошибки.

Вредоносное ПО распространяется автоматически.

В прошлом году исследователь безопасности Алекс Бирсан натолкнулся на идею, работая с другим исследователем Джастином Гарднером.

Гарднер поделился с Бирсаном файлом манифеста package.json из пакета npm, используемого внутри PayPal.

Бирсан заметил, что некоторые из пакетов файлов манифеста не присутствовали в общедоступном репозитории npm, а были вместо этого частными пакетами npm, созданными PayPal, которые используются и хранятся внутри компании.

Увидев это, исследователь задался вопросом, должен ли пакет с таким же именем существовать в общедоступном репозитории npm в дополнение к частному репозиторию NodeJS, какой из них получит приоритет?

Чтобы проверить эту гипотезу, Бирсан начал поиск имен частных внутренних пакетов, которые он мог найти в файлах манифестов в репозиториях GitHub или в CDN известных компаний, но не существовал в общедоступных репозиториях с открытым исходным кодом.

Затем исследователь начал создавать поддельные проекты с использованием тех же имен в репозиториях с открытым исходным кодом, таких как npm, PyPI и RubyGems.

Каждый пакет, опубликованный Бирсаном, создавался под его реальной учетной записью и явно имел заявление об отказе от ответственности, в котором говорилось: «Этот пакет предназначен для исследования безопасности и не содержит никакого полезного кода».

Бирсан вскоре понял, что если пакет зависимостей, используемый приложением, существует как в общедоступном репозитории с открытым исходным кодом, так и в вашей частной сборке, публичный пакет получит приоритет и будет извлечен вместо него - без каких-либо действий со стороны разработчика.

В некоторых случаях, как в случае с пакетами PyPI, исследователь заметил, что пакет с более высокой версией будет иметь приоритет независимо от того, где он находится.

Используя эту технику, Бирсан провел успешную атаку цепочки поставок против Microsoft, Apple, PayPal, Shopify, Netflix, Tesla, Yelp и Uber, просто опубликовав общедоступные пакеты с тем же именем, что и внутренние пакеты компании.

«Я считаю, что путаница в зависимости сильно отличается от типосквоттинга или брэнджекинга, так как не обязательно требует от жертвы какого-либо ручного ввода».

«Скорее, уязвимости или недостатки дизайна в автоматизированных инструментах сборки или установки могут привести к тому, что общедоступные зависимости будут ошибочно приняты за внутренние зависимости с тем же именем», - сказал Бирсан BleepingComputer в интервью по электронной почте.

Реконструкция и кража данных через DNS

Пакеты имели сценарии предварительной установки, которые автоматически запускали сценарий для извлечения идентифицирующей информации с машины, как только процесс сборки извлекал пакеты.

Зная, что его сценарии будут устанавливать соединения из корпоративных сетей, Бирсан решил использовать DNS для эксфильтрации данных, чтобы обойти обнаружение.

«Зная, что большинство возможных целей будут находиться глубоко внутри хорошо защищенных корпоративных сетей, я решил, что лучше всего использовать DNS-эксфильтрацию», - говорит Бирсан в своем блоге.

Фрагмент кода, показанный ниже, взят из сквотированного пакета npm " analytics-paypal», который теперь удален из npm. Однако, как исследователь безопасности в Sonatype, я смог получить его из наших архивов автоматического обнаружения вредоносных программ.

Этот скрипт запускается автоматически, как только будет извлечена зависимость «аналитика-пайпал» и появится код для выполнения DNS-запросов к dns.alexbirsan-hacks-paypal.com.

Обратный вызов, полученный от систем PayPal, затем предупредил бы исследователя о том, что IP-адрес, отправляющий запрос, принадлежит PayPal, а также имя пользователя и домашний каталог зараженной системы.

Получив такие обратные вызовы и в достаточной степени убедившись, что поддельный компонент исследователя успешно проник в корпоративную сеть,

Бирсан сообщал о своих выводах соответствующей компании и получал вознаграждение за обнаружение ошибок.

Заработано более $ 130 000 в виде баунти

В целом исследователю удалось заработать более 130 000 долларов США за счет программ поощрения ошибок и предварительно утвержденных механизмов тестирования на проникновение.

«Я считаю, что важно дать понять, что каждая организация, на которую было направлено это исследование, предоставила разрешение на тестирование своей безопасности либо через общедоступные программы поощрения ошибок, либо через частные соглашения. Пожалуйста, не пытайтесь проводить такой тест без разрешения, "предупреждает Бирсан.

За раскрытие информации Бирсаном Microsoft присудила ему самое высокое вознаграждение за обнаружение ошибок в размере 40 000 долларов и выпустила официальный документ по этой проблеме безопасности. Они идентифицируют эту проблему как CVE-2021-24105 для своего продукта Azure Artifactory.

Однако Microsoft сообщила Бирсану в электронном письме, что считает это недостатком дизайна в менеджерах пакетов.

«Хотя мы рассматриваем это как серьезную проблему безопасности, в конечном итоге она должна быть исправлена путем перенастройки инструментов установки и рабочих процессов, а не путем исправления чего-либо в самих репозиториях пакетов».

«Чтобы решить эту проблему, Microsoft внесла небольшие улучшения в артефакты Azure, чтобы гарантировать их использование в качестве надежного обходного пути».

«Тем не менее, мы считаем, что основной причиной этой проблемы является недостаток дизайна (а не ошибка) в диспетчерах пакетов, которые можно устранить только путем перенастройки», - заявил представитель Microsoft в электронном письме.

В заявлении для BleepingComputer Yelp подтвердил отчет исследователя и наградил его после исправления проблемы в течение дня.

«Через Yelp в программе ошибка-баунти, Алекс Бирсан помог нам определить уязвимость, которую мы немедленно заплатками в течение дня.»

«Мы стремимся работать с экспертами по безопасности, чтобы быть в курсе последних технологий безопасности, и полагаемся на нашу программу вознаграждения за ошибки, чтобы вознаграждать опытных исследователей безопасности, которые помогают улучшить системы и услуги Yelp», - сказал BleepingComputer представитель Yelp.

Apple сообщила BleepingComputer, что Бирсан получит вознаграждение в рамках программы Apple Security Bounty за ответственное раскрытие этой проблемы.

Принимая во внимание, что PayPal теперь публично раскрыл отчет Бирсана HackerOne, в котором упоминается сумма вознаграждения в размере 30 000 долларов.

Однако не все одобряли этические исследовательские усилия исследователя.

«Я думаю, что это [является], вероятно, достаточной причиной, чтобы не размещать эти проекты на PyPI», - утверждает Дастин Инграм, директор Python Software Foundation и сторонник разработчиков Google, который исследовал и удалил некоторые пакеты Бирсана из PyPI.

Потратив час на удаление этих пакетов, Ингрэм подчеркнул, что загрузка незаконных пакетов в PyPI ложится чрезмерным бременем на добровольцев, поддерживающих PyPI.

«В конечном итоге, если вы заинтересованы в защите пользователей от такого рода атак, есть более эффективные способы сделать это, которые защищают всю экосистему, а не только конкретный набор организаций с вознаграждением за ошибки», - добавил Ингрэм.

Ожидается, что количество атак будет расти, проблему сложно решить

Бирсан говорит, что с помощью этого исследования, охватывающего крупные организации, он уже информировал об этом типе атаки известные технологические компании, которые теперь внедрили некоторые меры по смягчению последствий в своей инфраструктуре. Однако исследователь считает, что предстоит еще многое сделать.

По-прежнему существует возможность повторного появления и роста таких атак, особенно на платформах с открытым исходным кодом, где нет простого решения для путаницы с зависимостями.

«В частности, я считаю, что поиск новых и умных способов утечки внутренних имен пакетов раскроет еще более уязвимые системы, а изучение альтернативных языков программирования и репозиториев для нацеливания откроет некоторую дополнительную поверхность атаки для ошибок путаницы зависимостей», - заключил исследователь в своем заключении. сообщение в блоге.

Sonatype выпустила сценарий на GitHub, который пользователи Nexus Repository Manager могут запустить, чтобы проверить, названы ли какие-либо их частные зависимости в честь существующих пакетов, присутствующих в общедоступных репозиториях npm, RubyGems и PyPI. Компании других менеджеров репозиториев артефактов могут использовать идентичные реализации.

BleepingComputer заранее связалась с компаниями, упомянутыми в этом отчете, включая Microsoft, Apple, PayPal, Shopify, Netflix, Tesla, Yelp, Tesla и Uber. Мы опубликовали заявления компаний, которые ответили раньше времени печати». ***(Ax Sharma. Researcher hacks over 35 tech firms in novel supply chain attack // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/researcher-hacks-over-35-tech-firms-in-novel-supply-chain-attack/). 09.02.2021).***

***

«Microsoft исправила ошибку, которая могла позволить злоумышленнику создавать специально созданные загрузки, приводящие к сбою Windows 10, просто открыв папку, в которую они были загружены.

В прошлом месяце мы сообщили об ошибке в драйвере мультиплексора консоли Windows 10, condrv.sys, которая вызвала синий экран смерти (BSOD) при попытке подключиться по следующему пути.

При подключении к устройству разработчики должны передать расширенный атрибут «прикрепить». Однако отсутствие проверки ошибок позволило вам получить доступ к пути без атрибута и вызвать сбой Windows.

Эта ошибка открыла множество потенциальных методов сбоя Windows, включая доступ к пути из адресной строки браузера, попытку назначить его букве диска с помощью 'net use' или создание специально созданного файла URL, который устанавливает свой значок на дорожка.

Хуже того, злоумышленники, которые получают доступ к системе, могут использовать его, чтобы заставить сбой взломанной системы, чтобы скрыть свои действия.

В рамках вторника патчей за февраль 2021 года Microsoft исправила эту ошибку и отследила ее как CVE-2021-24098 с описанием «Уязвимости, связанной с отказом в обслуживании драйвера консоли Windows».

Часто задаваемые вопросы Microsoft по уязвимости объясняют, как злоумышленники могут воспользоваться ошибкой.

"В случае атаки через Интернет злоумышленник может разместить веб-сайт (или использовать взломанный веб-сайт, который принимает или размещает предоставленный пользователем контент), который содержит специально созданный файл, предназначенный для использования этой уязвимости. Однако злоумышленник может нет способа заставить пользователя посетить веб-сайт».

«Вместо этого злоумышленник должен будет убедить пользователя щелкнуть ссылку, обычно с помощью соблазна в сообщении электронной почты или мгновенного обмена сообщениями, а затем убедить пользователя открыть специально созданный файл», - объясняет Microsoft CVE-2021-24098 страница уязвимости.

После установки обновления BleepingComputer может подтвердить, что уязвимость больше не может быть использована. Например, когда мы попытались назначить путь к диску f: с помощью команды net use, Windows 10 больше не вылетает…». ***(Lawrence Abrams. Microsoft fixes Windows 10 bug letting attackers trigger BSOD crashes // Bleeping Computer® (https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-windows-10-bug-letting-attackers-trigger-bsod-crashes/). 10.02.2021).***

***

«В Internet Explorer была обнаружена уязвимость нулевого дня, использовавшаяся в недавних северокорейских атаках на исследователей безопасности и уязвимостей.

В прошлом месяце Google сообщил, что хакерская группа Lazarus, спонсируемая государством Северной Кореи, проводила атаки социальной инженерии на исследователей безопасности.

Для выполнения своих атак злоумышленники создали тщательно продуманные образы «исследователей безопасности» в Интернете, которые затем будут использовать социальные сети для связи с известными исследователями безопасности для совместной работы над уязвимостями и разработками уязвимостей.

В рамках этого сотрудничества злоумышленники отправляли вредоносные проекты Visual Studio и ссылки на веб-сайты, на которых размещались наборы эксплойтов, которые устанавливали бэкдоры на компьютеры исследователей.

Microsoft также сообщила, что отслеживает атаку и видела, как Lazarus отправлял исследователям файлы MHTML, содержащие вредоносный javascript. Во время расследования сервер управления не работал, и Microsoft не могла исследовать дополнительные полезные данные.

Internet Explorer нулевого дня используется в атаках

Сегодня южнокорейская компания по кибербезопасности ENKI сообщила, что Lazarus нацелил исследователей безопасности из их команды с помощью файлов MHTML в этой кампании социальной инженерии.

Хотя они заявляют, что атаки не удались, они проанализировали полезные нагрузки, загруженные файлом MHT, и обнаружили, что он содержит эксплойт для уязвимости нулевого дня Internet Explorer.

Файл MHT / MHTML, также известный как MIME HTML, представляет собой специальный формат файла, используемый Internet Explorer для хранения веб-страницы и ее ресурсов в одном архивном файле.

MHT-файл, отправленный исследователям ENKI, содержал якобы эксплойт Chrome 85 RCE и назывался Chrome_85_RCE_Full_Exploit_Code.mht.

При открытии файла MHT / MHTML автоматически запускается Internet Explorer для отображения содержимого файла MHT. Если выполнение сценария было разрешено, ENKI сообщает, что вредоносный javascript загрузит две полезные нагрузки, одна из которых содержит нулевой день для Internet Explorer.

Этот эксплойт злоупотребляет ошибкой двойного освобождения в IE 11, позволяя злоумышленникам загружать список запущенных процессов, снимки экрана и сетевую информацию на свой сервер управления и контроля. Затем он загрузит и выполнит дополнительный вредоносный код с сервера C2 для выполнения.

ENKI сообщили BleepingComputer, что они сообщили об ошибке в Microsoft, и позже с ними связался сотрудник Microsoft с просьбой предоставить дополнительную информацию.

Генеральный директор Acros и соучредитель 0patch Митя Колсек сказал BleepingComputer, что он смог воспроизвести PoC нулевого дня Internet Explorer, о котором сообщает ENKI.

Основываясь на твитах других исследователей безопасности, ENKI сообщил BleepingComputer, что, по их мнению, другие исследователи знают об этом IE 11 нулевого дня.

Microsoft сообщила BleepingComputer, что они исследуют каждый отчет и предоставят обновления в будущем.

«Корпорация Майкрософт берет на себя обязательство клиентов исследовать сообщаемые проблемы безопасности, и мы как можно скорее предоставим обновления для затронутых устройств», - представитель Microsoft». ***(Lawrence Abrams. Hacking group also used an IE zero-day against security researchers // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/hacking-group-also-used-an-ie-zero-day-against-security-researchers/). 04.02.2021).***

***

«Публичное раскрытие атаки с повышением привилегий подробно описывает, как кибергруппа обошла песочницу браузера iframe с помощью вредоносных всплывающих окон PostMessage.

Подробная информация об уязвимости в браузере Apple Safari, обнародованная во вторник, описывает, как кибергруппа, известная как ScamClub, достигла 50 миллионов пользователей с помощью трехмесячной вредоносной рекламной кампании по распространению вредоносного ПО на мобильные браузеры iOS Chrome и macOS для настольных ПК.

Ошибка Safari, исправленная 2 декабря компанией Apple, использовалась в кампании злонамеренной рекламы, которая перенаправляла трафик на мошеннические сайты, которые отправляли жертвам подарочные карты, призы и вредоносное ПО. Пострадал браузер Safari от Apple, работающий на macOS Big Sur 11.0.1, и браузер Chrome на базе iOS от Google. Общей нитью является структура движка браузера Apple WebKit.

Согласно сообщению в блоге, опубликованному во вторник Элия Штейн, старшим инженером по безопасности, который обнаружил ошибку 22 июня 2020 года, атаки, которые исследователи Confiant Security приписывают ScamClub, использовали уязвимость в движке WebKit с открытым исходным кодом.

Он сообщает, что вредоносная кампания использовала уязвимость повышения привилегий, отслеживаемую как CVE-2021–1801. Штейн не сообщил, сколько людей, если таковые имеются, могли быть затронуты кампанией, или какие злонамеренные действия могли совершить злоумышленники после взлома. Как правило, основной целью атаки с повышением привилегий является получение неавторизованного доступа к целевой системе.

Что такое ScamClub?

ScamClub - это хорошо зарекомендовавшая себя кибергруппа, которая за последние три года захватила сотни миллионов сеансов браузера с помощью кампаний вредоносной рекламы, которые перенаправляют пользователей на мошенничество с взрослыми и подарочными картами.

До сегодняшнего дня группа наиболее известна масштабной кампанией 2018 года, в ходе которой 300 миллионов пользователей были перенаправлены на теневые фишинговые сайты, обслуживая контент для взрослых и мошенничество с подарочными картами.

Confiant назвал группу ScamClub из-за того, что преступник использовал несколько быстро меняющихся цепочек перенаправления, в конечном итоге выплевывая сомнительные предложения подарочных карт и контент для взрослых.

Исследователи отмечают, что ScamClub обычно использует стратегию «бомбардировки», чтобы наводнить системы доставки рекламы «огромным огромным спросом», а не пытаться скрыть свою гнусную деятельность.

«Они делают это на невероятно больших объемах в надежде, что небольшой процент проскальзывающих материалов нанесет значительный ущерб», - пояснил он.

Каковы подробности использования уязвимости WebKit в ScamClub?

В своем отчете во вторник Штейн сказал, что эта последняя кампания ScamClub перенаправляла пользователей на целевые страницы, предлагающие призы, такие как «Вы выиграли подарочную карту Walmart!» или «Вы выиграли iPhone!» «с весьма успешным эффектом, - писал он.

Только за последние 90 дней ScamClub произвел более 50 миллионов вредоносных показов, «поддерживая низкий базовый уровень активности, дополненный частыми маниакальными всплесками». По словам Штайна, за один день было показано до 16 миллионов затронутых объявлений.

Этот тип вектора атаки может быть трудным как для обычного человека, использующего Интернет, так и для бизнеса, учитывая потенциальное количество обслуживаемой вредоносной рекламы, отмечает Сарью Найяр, генеральный директор компании Gurucul, объединенной в области безопасности и анализа рисков.

«Подобные атаки могут быть проблемой для домашних пользователей, помимо поддержания их исправлений в актуальном состоянии, полагаясь на предоставленный интернет-провайдером или сторонний сервис для блокировки известных вредоносных доменов DNS», - сказала она в электронном письме Threatpost. «Организации сталкиваются с аналогичной проблемой из-за огромного количества вредоносной рекламы, но могут извлечь выгоду из использования тех же методов и аналитики безопасности, которые могут помочь идентифицировать вредоносные действия по их поведению».

Дневник эксплойта WebKit

Последняя полезная нагрузка ScamCard состоит из нескольких этапов, начиная с рекламного тега, который загружает вредоносную зависимость, размещенную в сети доставки контента, обычно «абсурдными способами запутываемой в попытке обойти черные списки URL-адресов», которые могут расширяться до тысяч строк кода. - написал Штейн.

Он сказал, что исследователи Confiant сузили свое расследование до четырех строк кода, которые в конечном итоге предупредили их об использовании ScamClub ошибки WebKit в своей кампании… обнаружив, что код отличался от типичной тактики злонамеренной рекламы, заключающейся в попытке «распылить множество попыток перенаправления» в одной полезной нагрузке, которая пытается выполнить перенаправление разными способами», - исследовали исследователи, создав простой HTML-файл, в котором реализован фрейм песочницы с перекрестным происхождением и кнопка, отправляющая их событие.

«Атрибут песочницы «allow-top-navigation-by-user-activate», который часто называют одним из наиболее важных инструментов в стратегии борьбы с вредоносной рекламой, теоретически должен предотвращать любое перенаправление, если не произойдет надлежащая активация», Стейн объяснил. «Активация в этом контексте обычно означает касание или щелчок внутри рамки».

Если бы это было так, то доказательство концепции Confiant не могло бы перенаправить страницу. Тем не менее, это произошло, что доказало исследователям, что использование ScamClub «обхода песочницы iframe с длинным хвостом» было связано с ошибкой браузера, которая оказалась в WebKit». ***(Elizabeth Montalbano. Details Tied to Safari Browser-based 'ScamClub' Campaign***

Revealed // Threatpost (https://threatpost.com/safari-browser-scamclub-campaign-revealed/164023/). 17.02.2021).

***

«Критический недостаток кибербезопасности SAP может привести к компрометации приложения, используемого предприятиями электронной коммерции.

SAP предупреждает о критической уязвимости в своей платформе SAP Commerce для предприятий электронной коммерции. В случае эксплуатации уязвимость может позволить удаленное выполнение кода (RCE), что в конечном итоге может поставить под угрозу или нарушить работу приложения.

SAP Commerce систематизирует данные, например, информацию о продуктах, для распространения по нескольким каналам. Это может дать предприятиям преимущество в решении сложных вопросов управления цепочкой поставок.

Уязвимость (CVE-2021-21477) затрагивает SAP Commerce версий 1808, 1811, 1905, 2005 и 2011. Она занимает 9,9 балла из 10 по шкале CVSS, что делает ее критической по серьезности.

«Учитывая присвоенный рейтинг CVSS 9,9 и потенциальное влияние на приложение, настоятельно рекомендуется как можно скорее уменьшить уязвимость», - сказал Томас Фрич из Onapsis во вторник.

Что такое правила SAP Commerce Drools?

Недостаток позволяет определенным пользователям с «необходимыми привилегиями» редактировать правила Drools. Drools - это механизм, который составляет механизм правил для SAP Commerce. Цель Drools - определить и выполнить набор правил, которые могут использоваться предприятиями для управления сложными сценариями принятия решений.

Недостаток проистекает из правила в Drools, которое содержит атрибут ruleContent. Этот атрибут предоставляет возможности для написания сценариев. Юрисдикция над ruleContent обычно закрепляется за пользователями с высокими привилегиями, такими как администраторы, сказал Фрич.

Однако «из-за неправильной настройки разрешений пользователей по умолчанию, которые поставляются с SAP Commerce, несколько пользователей и групп пользователей с более низкими привилегиями получают разрешения на изменение содержимого правила DroolsRule и, таким образом, получают непреднамеренный доступ к этим средствам создания сценариев», - сказал Фритч.

Удаленное выполнение кода в SAP Commerce

Это означает, что злоумышленник с таким более низким уровнем привилегий может внедрить вредоносный код в сценарии правил Drools, что приведет к RCE и компрометации базового хоста. И, в конечном итоге, это позволяет киберпреступникам нарушить «конфиденциальность, целостность и доступность приложения», - сказал Фрич.

Вышел патч; однако, по словам Фрича, исправления уязвимости касаются только разрешений по умолчанию при инициализации новой установки SAP Commerce.

«Для существующих установок SAP Commerce требуются дополнительные действия по исправлению вручную», - сказал он. «Хорошая новость заключается в том, что для существующих установок эти шаги по исправлению вручную можно использовать в качестве полного обходного пути для установок SAP Commerce, которые не могут своевременно установить последние выпуски исправлений».

Другие важные версии SAP Cybersecurity Releases

Обновление уязвимости было одним из семи примечаний по безопасности, выпущенных SAP во вторник. Остальные шесть выпусков были обновлениями ранее выпущенных примечаний по безопасности Patch Tuesday.

Один из них получил 10-е место по шкале CVSS и решал проблемы безопасности в управлении браузером для Google Chromium, который поставляется с бизнес-клиентом SAP. Это влияет на бизнес-клиент SAP версии 6.5. Конкретное назначение CVE для этой уязвимости и другие подробности не были доступны.

Еще один недостаток критической степени серьезности, который был ранее опубликован и обновлен во вторник, включал несколько недостатков (CVE-2021-21465) в SAP Business Warehouse, продукте для хранения данных, основанном на платформе SAP NetWeaver ABAP, который собирает и хранит данные.

«Интерфейс базы данных BW позволяет злоумышленнику с низкими привилегиями выполнять любые созданные запросы к базе данных, обнажая внутреннюю базу данных», - сообщает Miter Corporation. «Злоумышленник может включить свои собственные команды SQL, которые база данных будет выполнять без должной очистки ненадежных данных, что приведет к уязвимости SQL-инъекции, которая может полностью скомпрометировать уязвимую систему SAP».

Патч вторник обновлений безопасности

Исправления уязвимостей производятся во время загруженной недели после исправлений во вторник. Microsoft исправила девять критических ошибок безопасности в своих обновлениях, выпущенных во вторник за февраль, а также одну уязвимость с серьезным рейтингом, которая активно эксплуатируется в дикой природе.

Adobe предупредила о критической уязвимости, которая использовалась в дикой природе в «ограниченных атаках» для пользователей Adobe Acrobat Reader в Windows.

Кроме того, Intel выпустила исправления для пяти уязвимостей высокой степени серьезности в своих графических драйверах. Злоумышленники могут использовать эти недостатки для запуска ряда вредоносных атак, таких как повышение своих привилегий, кража конфиденциальных данных или запуск атак типа «отказ в обслуживании». ***(Lindsey O'Donnell. SAP Commerce Critical Security Bug Allows RCE // Threatpost (https://threatpost.com/sap-commerce-critical-security-bug/163822/). 10.02.2021).***

***

«Исследовательское тестирование 30 мобильных медицинских приложений для врачей показало, что все они имеют уязвимые API.

По данным исследователей, около 23 миллионов пользователей мобильных приложений здравоохранения (mHealth) подвергаются атакам на интерфейс

программирования приложений (API), которые могут раскрыть конфиденциальную информацию.

Вообще говоря, API - это посредник между приложениями, который определяет, как они могут общаться друг с другом, и позволяет им обмениваться информацией. Исследователь Алисса Найт и Approov пытались взломать API 30 различных поставщиков приложений mHealth, при этом договорились, что она не будет идентифицировать уязвимых. Оказывается, все они в той или иной степени были уязвимы.

Среднее количество загрузок для каждого протестированного приложения составило 772 619 раз.

Согласно итоговому отчету Approov, из 30 проанализированных популярных приложений mHealth 77 процентов содержали жестко запрограммированные ключи API, которые позволили бы злоумышленнику перехватить этот обмен информацией, срок действия некоторых из которых не истекает. Семь процентов из них принадлежали сторонним платежным системам, которые прямо предупреждают о недопустимости жесткого кодирования своих секретных ключей в виде обычного текста.

Еще 7 процентов содержали жестко запрограммированные имена пользователей и пароли.

Но это еще не все: более четверти (27 процентов) протестированных мобильных приложений не имеют защиты от обфускации кода от обратного проектирования; и у всех без исключения не было закрепления сертификатов, которое предотвращало бы атаки «мужчина (или женщина) в середине» (MITM) для перехвата сообщений для наблюдения и управления записями.

Кроме того, полные 50 процентов протестированных API не аутентифицировали запросы с помощью токенов.

И, наконец, если можно получить доступ к записям одного пациента, часто можно получить доступ ко многим другим без разбора: 100 процентов протестированных конечных точек API были уязвимы для атак с нарушением авторизации на уровне объектов (BOLA), что позволило исследователю просматривать личную информацию о здоровье (PHI). и личная информация (PII) для пациентов, которая не была привязана к учетной записи врача-исследователя.

В контексте отчета говорится, что в крупных магазинах приложений доступно более 318 000 приложений.

Медицинские записи привлекают киберпреступников

Пандемия вынуждает больницы и поставщиков медицинских услуг все больше полагаться на приложения мобильного здравоохранения. Но анализ показывает, что они часто уязвимы для злоумышленников, оставляя критически важную и ценную информацию о здоровье, ожидающую, когда ее украдут.

Как объяснил Найт Threatpost, безопасность мобильных приложений для здоровья усугубляет безумное стремление к инновациям, а во-вторых, к безопасности. И теперь пора, чтобы служба безопасности наверстала упущенное, прежде чем произойдет серьезное нарушение, добавила она.

Между тем у злоумышленников есть большой финансовый стимул для нацеливания на эти API мобильного здравоохранения. Найт указал, что, хотя

обычная ставка для киберпреступников за номер социального страхования составляет 1 доллар, а номер кредитной карты продается примерно за 110 долларов, большие деньги находятся в полной медицинской документации, которая составляет около 1000 долларов за штуку.

«Эта растущая поверхность для атак быстро привлекает внимание транснациональных преступных синдикатов, желающих заблокировать их, чтобы вымогать платежи у владельцев данных и продавать их по самой высокой цене», - написал Найт в своем отчете.

Что такое основная угроза для приложений мобильного здравоохранения?

По словам Найт, BOLA (также известная как Insecure Direct Object Reference, или IDOR) является наиболее распространенным вектором злоупотреблений для API-интерфейсов mHealth, отметив, что неслучайно недавно опубликованный OWASP список основных угроз API помещает эти типы уязвимостей на первое место.

«Проще говоря, уязвимость BOLA позволяет злоумышленнику заменить идентификатор ресурса на идентификатор другого», - пояснил Найт. «Когда идентификатор объекта может быть напрямую вызван в URI, он открывает конечную точку до перечисления идентификаторов, что позволяет злоумышленнику читать объекты, которые ему не принадлежат. Эти открытые ссылки на внутренние объекты реализации могут указывать на что угодно, будь то файл, каталог, запись базы данных или ключ».

Лабораторные атаки BOLA, проведенные Найт, взломали 100% приложений, которые она тестировала, предоставив ей теоретический доступ к загружаемым полным записям пациентов, включая результаты лабораторных исследований, рентгеновские снимки, анализ крови, семейный анамнез, даты рождения, номера социального страхования. и больше.

Авторизация API или аутентификация

Найт объяснил Threatpost, что когда дело доходит до API, директорам по информационной безопасности и службам безопасности следует подумать о различии между аутентификацией и авторизацией.

Найт использовал аналогию с охраной в ночном клубе.

В сценарии только с авторизацией вышибала (авторизатор) проверяет идентификаторы и определяет, кому разрешено входить в панель. Так что внутри бармен может предположить, что любой, кто подходит к бару и заказывает напиток, употребляет алкоголь законно.

Но в сценарии аутентификации есть две проверки.

Вышибала проверяет удостоверения личности и выдает браслеты тем, кому разрешено пить. Оказавшись в баре, бармен (аутентификатор) ищет браслет как дополнительный элемент проверки. Двойная проверка бармена подтверждает, что человеку не только разрешено находиться в баре, но также удостоверяется его личность, чтобы убедиться, что им обоим разрешено находиться в баре и разрешено употреблять алкоголь.

Найт объяснил, что API работают примерно так же. Половина API-интерфейсов mHealth, которые она тестировала для этого отчета, не аутентифицировали запросы с помощью токенов.

«Типы аутентификации в API включают ключи API, длинную строку случайных чисел и символов, сгенерированную конечной точкой API, которая предоставляет доступ любому, кто передает его в заголовке авторизации запроса; Базовая аутентификация, при которой имя пользователя и пароль используются для аутентификации человека; JSON Web Tokens (JWT) и OAuth, который использует токены вместо обмена учетными данными; OAuth2, который обменивает имя пользователя и пароль на токен; SMART, который все чаще становится реализацией OAuth в здравоохранении; и OpenID Connect», - сказал Найт. «Существуют также другие методы аутентификации, такие как реализация многофакторной аутентификации с помощью сторонних решений».

Внедрение лучшей кибербезопасности мобильного здравоохранения

Дэвид Стюарт, основатель и генеральный директор Approov, объяснил, что существующие стандарты безопасности не подходят для устранения растущих угроз безопасности мобильных приложений для здоровья. Компаниям нужно делать больше.

«Эти результаты неутешительны, но вовсе не удивительны», - сказал Стюарт. «Дело в том, что ведущие разработчики и их корпоративные и организационные клиенты постоянно не осознают, что API-интерфейсы, обслуживающие удаленных клиентов, таких как мобильные приложения, нуждаются в новой специальной парадигме безопасности.»

Он подчеркнул, что организации здравоохранения должны понимать, что API-интерфейсы - это открытая дверь для злоумышленников, особенно на прибыльном рынке PHI.

«Поскольку очень мало организаций развертывают средства защиты для API, которые гарантируют, что только подлинные экземпляры мобильных приложений могут подключаться к внутренним серверам, эти API являются открытой дверью для злоумышленников и представляют собой настоящий кошмар для уязвимых организаций и их пациентов», - сказал Стюарт». ***(Becky Bracken. mHealth Apps Expose Millions to Cyberattacks // Threatpost (https://threatpost.com/mhealth-apps-millions-cyberattacks/163966/). 12.02.2021).***

***

«На прошлой неделе специалисты компании Qualys обнародовали информацию о проблеме в sudo, которой был присвоен идентификатор CVE-2021-3156 и название Baron Samedit. Тогда сообщалось, что баг, связанный с переполнением хипа, затрагивает большинство дистрибутивов Linux и может использоваться злоумышленником (уже имеющим хотя бы низкопривилегированный доступ к системе) для получения root-доступа.

Однако эксперты Qualys тестировали проблему только на Ubuntu, Debian и Fedora, а также писали об опасности для UNIX-систем. Теперь же ИБ-специалист и глава Hacker House Мэттью Хики (Matthew Hickey) сообщил в Twitter, что уязвимости Baron Samedit подвержена и macOS (в том числе самых последних версий), которая тоже укомплектована sudo.

Хики пишет, что в операционной системе Apple эксплуатировать CVE-2021-3156 можно с некоторыми изменениями, но баг точно так же может использоваться для получения root-доступа.

«Чтобы спровоцировать ошибку, вам просто нужно перезаписать argv[0] или создать символическую ссылку, которая подвергнет ОС той же локальной root-уязвимости, от которой на прошлой неделе страдали пользователи Linux», — объясняет эксперт.

Выводы Хики уже подтвердили такие известные ИБ-эксперты, как Патрик Уордл (Patrick Wardle, один из ведущих специалистов в мире по безопасности macOS) и Уилл Дорманн (Will Dormann, эксперт CERT в Университете Карнеги-Меллона).

Патча для macOS пока нет, но разработчикам Apple уже сообщили о баге, и они уже расследуют сообщения экспертов». ***(Мария Нефёдова. Недавно обнаруженный баг в sudo затрагивает macOS // Хакер (https://xakep.ru/2021/02/03/baron-samedit-macos/). 03.02.2021).***

***

«Команда специалистов из ИБ-компании FireEye проанализировала шлюз для солнечных электростанций и выявила ряд уязвимостей, которые могут оказаться весьма полезными для злоумышленников.

Объектом изучения стало решение ConnectPort X2e производства Digi International, а точнее версия устройства предлагаемая компанией Tesla под брендом SolarCity. Для справки, Tesla приобрела производителя солнечных панелей SolarCity в 2016 году.

ConnectPort X2e представляет собой программируемый шлюз для домашних и небольших коммерческих солнечных установок, который, как правило, используется для считывания данных с солнечного инвертора и подключения к облачным приложениям.

В ходе исследования специалисты обнаружили две уязвимости (CVE-2020-9306 и CVE-2020-12878). Первая связана с наличием вшитых учетных данных, а вторая представляет собой уязвимость повышения привилегий, обе проблемы получили высокий уровень опасности.

Как пояснили в FireEye, атакующий с сетевым доступом к целевому устройству может проэксплуатировать вышеуказанные уязвимости, получить доступ с правами суперпользователя и перехватить контроль над устройством. Скомпрометировав шлюз, хакер может установить бэкдор и получить постоянный доступ к домашней или корпоративной сети.

Как правило, шлюз ConnectPort X2e защищен «местным» межсетевым экраном и осуществить удаленные атаки на него - сложная задача, за исключением случаев, когда пользователь намеренно открывает доступ к устройству из интернета.

Специалисты проинформировали Digi International и Tesla о найденных уязвимостях, проблемы уже исправлены…» ***(Эксперты рассказали, как шлюзы для солнечных установок могут использоваться хакерами // SecurityLab.ru (https://www.securitylab.ru/news/516737.php). 18.02.2021).***

***

«Разработчики OpenSSL выпустили исправления для трех уязвимостей в своем проекте, эксплуатация двух из которых позволяет осуществлять атаки типа «отказ в обслуживании» (DoS).

Наиболее опасной проблемой (CVE-2021-23841) является уязвимость разыменования нулевого указателя, которая может привести к сбою и состоянию «отказа в обслуживании». Она связана с функцией (X509_issuer_and_serial_hash), которая никогда не вызывается непосредственно самим OpenSSL и затрагивает только приложения, использующие функцию напрямую с сертификатами, полученными из ненадежных источников.

Исследователь безопасности из Google Project Zero Тэвис Орманди (Tavis Ormandy) сообщил о проблеме, и разработчики OpenSSL исправили ее в версии OpenSSL 1.1.1j. В данной версии также была устранена уязвимость целочисленного переполнения (CVE-2021-23840), которая также может привести к сбою в работе.

Специалисты из компании Trustwave сообщили о другой проблеме (CVE-2021-23839) в проекте OpenSSL — серверы, использующие версию OpenSSL 1.0.2, уязвимы к атакам с откатом версии SSL. Однако атака может быть запущена только против определенных конфигураций, и уязвимость не затрагивает версию OpenSSL 1.1.1. Проблема была исправлена в версии 1.0.2y, однако данная версия OpenSSL больше не поддерживается, поэтому обновление доступно только для клиентов с премиум-поддержкой». ***(В проекте OpenSSL исправлены три опасные уязвимости // SecurityLab.ru (https://www.securitylab.ru/news/516688.php). 17.02.2021).***

***

«Устройства сейсмического мониторинга, подключенные к интернету, уязвимы для кибератакам, в результате которых может быть нарушен процесс сбора и обработки данных. Незашифрованные данные, незащищенные протоколы и слабые механизмы аутентификации пользователей являются одними из самых больших проблем, которые делают сейсмологические сети уязвимыми ко взломам, сообщил Майкл Самиос из Афинской национальной обсерватории.

Современные сейсмические станции теперь реализованы как IoT-станции с физическими устройствами, которые подключаются и обмениваются данными с другими устройствами и системами через интернет. Эксперты выявили ряд проблем в ходе экспериментальных атак на сейсмографы, акселерографы и приемники спутниковой системы навигации (GNSS) от различных производителей.

«Похоже, что большинство сейсмологов и сетевых операторов не знают об уязвимостях в своих IoT-устройствах и потенциальном риске, которому подвергаются их сети мониторинга», — сказал Самиос.

Эксплуатация уязвимостей позволяет злоумышленникам изменять геофизические данные, замедлять передачу и обработку информации или выдавать ложные сигналы тревоги в системах раннего предупреждения о землетрясениях, в результате чего население теряет доверие к сейсмическому мониторингу и потенциально могут повлиять на аварийные и экономические меры.

В рамках экспериментов исследовательская группа также смогла перехватить сейсмологические данные, передаваемые через службу передачи данных SeedLink, используемую многими сейсмологами. По словам Самиоса, SeedLink может не обладает некоторыми необходимыми протоколами шифрования и аутентификации для обеспечения безопасности данных». ***(Устройства сейсмического мониторинга уязвимы к DoS-атакам // SecurityLab.ru (https://www.securitylab.ru/news/516662.php). 17.02.2021).***

***

«Ошибка переполнения буфера критической степени серьезности, влияющая на IBM Integration Designer, может позволить удаленным злоумышленникам выполнить код.

IBM исправила критическую ошибку переполнения буфера, которая влияет на набор инструментов Big Blue Integration Designer, который помогает предприятиям создавать бизнес-процессы, объединяющие приложения и данные. В случае эксплуатации уязвимость может сделать возможным удаленное выполнение кода.

Недостаток (CVE-2020-27221) имеет базовую оценку CVSS 9,8 из 10, что делает его критическим по серьезности. Это происходит из-за проблемы в версиях 7 и 8 среды выполнения Java (JRE), которая используется набором инструментов IBM Integration Designer.

JRE - это программный уровень, который работает поверх операционной системы (ОС) компьютера и позволяет Java беспрепятственно работать в любой системе, независимо от ее ОС.

Что такое ошибка переполнения буфера?

Недостаток - ошибка переполнения буфера на основе стека. Это класс уязвимости, при котором область памяти процесса, используемая для хранения динамических переменных (куча), может быть перегружена.

«Отправив слишком длинную строку, удаленный злоумышленник может переполнить буфер и выполнить произвольный код в системе или вызвать сбой приложения», - говорится в сообщении IBM по безопасности в понедельник.

Ошибка возникает, когда виртуальная машина (ВМ) или собственный интерфейс Java преобразует символы из UTF-8 в кодировку платформы. Java Native Interface - это среда программирования, которая позволяет Java-коду, запущенному в Java VM, вызывать собственные приложения и библиотеки, написанные на других языках.

IBM не предоставила дополнительной информации о том, какие привилегии понадобятся злоумышленнику, куда им нужно будет отправить строку или начальный вектор атаки.

Затронуто IBM Integration Designer

В частности, CVE-2020-27221 существует в Eclipse OpenJ9, высокопроизводительной масштабируемой реализации виртуальной машины Java, полностью совместимой с JRE.

«Внесенная IBM в основу Eclipse, JVM OpenJ9 лежит в основе IBM SDK, Java Technology Edition, который является основным компонентом многих программных продуктов IBM Enterprise», - сообщает IBM.

Это касается IBM Integration Designer версий 8.5.7, 19.0.0.2, 20.0.0.1 и 20.0.0.2, которые используют JRE версий 7 и 8. Об уязвимости впервые было сообщено 16 декабря через Eclipse Foundation, которое является глобальным сообществом участников Eclipse, занимающихся разработкой программного обеспечения с открытым исходным кодом. Здесь можно найти исправление для каждой уязвимой версии IBM Integration Designer.

Была исправлена другая уязвимость (CVE-2020-14782), возникшая из-за реализации JRE в IBM Integration Designer. Эта «неуказанная» уязвимость существовала в Java SE и была связана с компонентом «Библиотеки». Однако, по словам IBM, это «не повлияло на конфиденциальность, не повлияло на целостность и не повлияло на доступность».

Серьезные недостатки IBM Planning Analytics Workspace

IBM также исправила множество серьезных недостатков в своем IBM Planning Analytics Workspace; веб-интерфейс для IBM Planning Analytics, который предоставляет интерфейс для создания и анализа контента. Недостатки существуют, в частности, в версии 61 локальной версии 2.0 для Planning Analytics Workspace.

Три уязвимости существуют в Node.js, кроссплатформенной среде выполнения JavaScript с открытым исходным кодом для разработки серверных и сетевых приложений, которая используется в IBM Planning Analytics. Эти недостатки включают уязвимость отказа в обслуживании (CVE-2020-8251); сбой при передаче HTTP-запросов (CVE-2020-8201); и ошибка переполнения буфера (CVE-2020-8252).

Другой недостаток (CVE-2020-25649) существует в FasterXML Jackson Databind, используемом для преобразования JSON в обычный старый объект Java (POJO) и обратно с помощью средства доступа к свойствам или аннотаций.

По словам IBM, уязвимость «может обеспечить более слабую, чем ожидалось, безопасность, вызванную отсутствием должной защиты расширения объекта». «Удаленный злоумышленник может использовать эту уязвимость для запуска атак на внешний объект XML (XXE), чтобы повлиять на целостность данных».

IBM продолжает кампанию по исправлению недостатков безопасности

IBM ранее выпускала различные исправления уязвимостей, в том числе в Spectrum Protect Plus в сентябре. Это инструмент безопасности Big Blue, который используется под брендом программного обеспечения для хранения данных Spectrum. Бреши могут использоваться удаленными злоумышленниками для выполнения кода в уязвимых системах…». ***(Lindsey O'Donnell. IBM Squashes Critical Remote Code-Execution Flaw // Threatpost (https://threatpost.com/ibm-critical-remote-code-execution-flaw/164187/). 23.02.2021).***

***

«Пользователи Twitter обнаружили уязвимость в новом алгоритме, с помощью которой метку «получено путем взлома» (obtained through hacking) можно добавлять к произвольным твитам.

На прошлой неделе в Twitter появился новый маркер «получено путем взлома», который соцсеть использует для обозначения публикаций, созданных на основе утечек и документов, полученных в результате взлома.

По словам старшего редактора The Verge Тома Уоррена (Tom Warren), для того чтобы воспользоваться уязвимостью и обойти алгоритм, нужно вставить в пост ссылку на материал, базирующийся на утечке. В таком случае Twitter будет считать его ненадежным источником и отметит его с помощью соответствующего маркера.

Метод воспроизводится как в iOS- и Android-приложениях Twitter, так и в web-версии. Если пользователь попытается поставить «Нравится» под такой публикацией на Android-устройстве, может произойти сбой (но только в том случае, если ссылка была создана преднамеренно).

Администрация соцсети пока не комментирует проблему, и когда она будет исправлена (и будет или исправлена вообще), неизвестно». ***(Уязвимость в Twitter позволяет маркировать произвольные твиты как утечки // SecurityLab.ru (https://www.securitylab.ru/news/516921.php(. 25.02.2021).***

***

Технічні та програмні рішення для протидії кібернетичним загрозам

«Год назад Forrester задокументировал новую модель безопасности и сетей, которая стала набирать популярность на рынке. В результате Forrester недавно опубликовал свое исследование в новом отчете, в котором представлена модель Zero Trust Edge для безопасности и сетевых служб. На рынке существует похожее название «Secure Access Services Edge» (SASE) для описания той же модели. Мы делаем акцент на нулевом доверии.

Компания Forrester является сторонником этой модели по нескольким причинам. Но основная из них заключается в следующем: Интернет был разработан с учетом требований безопасности. Должны ли мы, как технологи, просто ожидать, что каждая организация в мире просто присоединится к ней напрямую и надеяться, что у них все получится? В течение 25 лет мы просто накладывали пластыри поверх пластырей, надеясь остановить кровотечение из системы кибербезопасности, но бойня с каждым годом становится все хуже. Модель Zero Trust Edge (ZTE) - это более безопасный выход в Интернет для физических местоположений организаций и удаленных сотрудников.

Сеть ZTE - это виртуальная сеть, охватывающая Интернет и доступная напрямую из любого крупного города мира. Он использует Zero Trust Network Access (ZTNA) для аутентификации и авторизации пользователей, когда они подключаются к нему и через него. Если эти пользователи получают доступ к

корпоративным службам, таким как локальное приложение или Office 365, они могут даже редко «касаться» Интернета, за исключением безопасного туннелирования через него, и они, безусловно, будут держаться подальше от плохих районов города.

ТАКТИКА ПРОТИВ. СТРАТЕГИИ

Многие предприятия смотрят на эту модель, чтобы тактически решить конкретную проблему: обеспечить безопасность удаленной рабочей силы. Эти организации понимают, что приобретение дополнительных лицензий на VPN во время блокировки COVID-19 было лишь временной мерой, чтобы люди могли работать. Теперь они ищут решение ZTNA.

У всех поставщиков ZTE есть ZTNA, потому что это основная служба безопасности их стека. Как только предприятия начинают общаться с такими поставщиками, как Zscaler, Akamai или Netskope, они понимают, что есть больше сервисов безопасности, которые они могут использовать в качестве услуги, и теперь они уговаривают себя в стратегии ZTE.

В будущем, после интеграции в стек других технологий, таких как SWG, CASB и DLP, организации будут стремиться пропускать весь свой сетевой трафик через эти сети ZTE. И именно здесь группы безопасности и сети должны будут работать вместе, потому что унаследованные локальные сети неоднородны, а миграция гигантских центров обработки данных или 12-этажных больниц с использованием программно определяемой глобальной сети (SD-WAN) в качестве транспортного средства в ZTE сети будет проблемой.

Решим тактическую задачу, удаленный персонал, сначала с ZTNA. Далее мы перейдем к более серьезным проблемам безопасности. И наконец, обратимся к сети. В конце концов, удаленные пользователи, розничные филиалы, удаленные офисы, фабрики и центры обработки данных будут подключены к сетям ZTE, которые будут использовать подходы и технологии Zero Trust для аутентификации, дезинфекции и мониторинга соединений через сеть, в Интернет и общедоступные облака». ***(Take security to the Zero Trust Edge // ZDNet (https://www.zdnet.com/article/take-security-to-the-zero-trust-edge/).19.02.2021).***

***

«Испанский студент выпустил бесплатную утилиту для дешифрования, которая может помочь жертвам программы-вымогателя Avaddon бесплатно восстановить свои файлы.

Опубликованный на GitHub Хавьером Юсте, студентом Университета Рей Хуана Карлоса в Мадриде, AvaddonDecrypter работает только в тех случаях, когда жертвы не выключили свои компьютеры.

Инструмент работает, сбрасывая ОЗУ зараженной системы и просматривая содержимое памяти в поисках данных, которые можно было бы использовать для восстановления исходного ключа шифрования программы-вымогателя.

Если будет восстановлено достаточно информации, этот инструмент можно будет использовать для расшифровки файлов и помощи жертвам в восстановлении после атак Avaddon без необходимости платить выкуп.

БАНДА АВАДДОНА ИСПРАВЛЯЕТ СВОЙ КОД

Но хотя выпуск инструмента, скорее всего, поможет прошлым жертвам, он не поможет компаниям, которые станут жертвами новых атак Avaddon.

Это потому, что выпуск инструмента не остался незамеченным. В сообщении на форуме в среду банда Avaddon сообщила, что она также узнала о дешифраторе Юсте и уже развернула обновления своего кода, фактически сводя на нет возможности инструмента.

Реакция команды Avaddon отражает то, как команда вымогателей Darkside также ответила на выпуск аналогичного дешифратора для своего собственного штамма в прошлом месяце, в январе.

В конце концов, выпуск обеих утилит дешифрования оказал очень ограниченное влияние. Хотя некоторые жертвы смогли расшифровать файлы, как только о существовании инструмента дешифрования стало известно, банды вымогателей проанализировали, как эти инструменты работают, и исправили свой код в течение нескольких дней.

Выпуск этих двух инструментов, а также сообщение в блоге голландской охранной фирмы Eye Control, показывающее, как жертвы могут оправиться от атак с помощью программы-вымогателя Data Doctor, снова возродили многолетний разговор в индустрии кибербезопасности о том, как утилиты дешифрования должны быть обработаны и предоставлены жертвам.

Несколько видных исследователей в области безопасности, которые долгое время помогали жертвам программ-вымогателей с середины 2010-х годов, вновь заявили о своем мнении за последние два месяца, подчеркнув тот факт, что служебные программы для дешифрования, использующие ошибки шифрования программ-вымогателей, должны быть конфиденциальными и распространяться среди жертв через непубличные каналы, а не через рекламу в Интернете.

Более того, даже если такие инструменты должны быть обнародованы, не должно быть никаких технических деталей, сопровождающих выпуск инструмента, деталей, которые, очевидно, помогут злоумышленникам также исправить свой собственный код.

С другой стороны, утилиты дешифрования, построенные на основе главных ключей дешифрования, полученных с серверов злоумышленников, могут быть опубликованы в Интернете, поскольку авторы программ-вымогателей мало что могут сделать с этими инструментами.

В общем, глядя на то, как группы Avaddon и Darkside отреагировали - исправив свои схемы шифрования в течение нескольких дней, - трудно спорить с аргументами, высказанными в Интернете за последние два месяца, а именно, что некоторые инструменты дешифрования никогда не должны становиться общественным достоянием». **(Catalin Cimpanu. Free decrypter released for Avaddon ransomware victims... aaand, it's gone! // ZDNet (https://www.zdnet.com/article/free-decrypter-released-for-avaddon-ransomware-victims-aaand-its-gone/). 11.02.2021).**

***

«Атаки на уязвимые компьютерные сети и кибер-инфраструктуру - часто называемые атаками нулевого дня - могут быстро преодолеть

традиционную защиту, что приведет к ущербу в миллиарды долларов и потребует недель ручной работы по установке исправлений, чтобы укрепить системы после вторжения.

Теперь команда исследователей под руководством Пенсильванского университета использовала подход машинного обучения, основанный на методе, известном как обучение с подкреплением, для создания адаптивной киберзащиты от этих атак.

По словам Минхуэй Чжу, доцента электротехники и информатики и соавтора Института вычислений и данных, команда разработала этот адаптивный метод, основанный на машинном обучении, для устранения текущих ограничений метода обнаружения и реагирования на кибератаки так называемая защита движущейся цели, или МПД.

«Эти адаптивные методы ручной защиты целей могут динамически и проактивно перенастраивать развернутые средства защиты, что может увеличить неопределенность и сложность для злоумышленников во время окон уязвимости», - сказал Чжу. «Однако существующие методы МПД страдают двумя ограничениями. Во-первых, ручной выбор может занять очень много времени. Во-вторых, выбранные вручную конфигурации могут быть не самым рентабельным методом решения этой проблемы».

Типичные ответы на атаку могут занять до 15 дней, что может потребовать значительных средств и ресурсов для организации, по словам исследователей, опубликовавших свои выводы в ACM Transactions on Privacy and Security.

Чжу сказал, что атаки нулевого дня являются одной из самых опасных угроз для компьютерных систем и могут нанести серьезный и долговременный ущерб. Например, атака программы-вымогателя WannaCry, произошедшая в мае 2017 года, была нацелена на более чем 200 000 компьютеров Windows в 150 странах и нанесла ущерб на сумму от 4 до 8 миллиардов долларов.

Подход команды основан на обучении с подкреплением, которое, наряду с обучением с учителем и без учителя, является одной из трех основных парадигм машинного обучения. По словам исследователей, обучение с подкреплением - это способ, с помощью которого лицо, принимающее решения, может научиться делать правильный выбор, выбирая действия, которые могут максимизировать вознаграждение, балансируя эксплуатацию - используя прошлый опыт - и исследование - пробуя новые действия, согласно Пэн Лю, Раймонду. Г. Тронзо, доктор медицинских наук, профессор кибербезопасности Колледжа информационных наук и технологий.

«Лицо, принимающее решения, изучает оптимальную политику или действия через непрерывное взаимодействие с базовой средой, которая частично неизвестна», - сказал Лю. «Таким образом, обучение с подкреплением особенно хорошо подходит для защиты от атак нулевого дня, когда критическая информация - цели атак и расположение уязвимостей - недоступна».

Исследователи протестировали свой алгоритм обучения с подкреплением в сети из 10 машин. Они добавили, что, хотя сеть из 10 компьютеров может показаться не очень большой, на самом деле она более чем достаточно устойчива для теста. В установку также входили веб-сервер и почтовый сервер, сервер шлюза,

сервер SQL, сервер DNS и сервер администратора. Был установлен брандмауэр для предотвращения доступа к внутренним хостам. Исследователи также выбрали уязвимости, которые могут привести к множеству сценариев атаки для теста.

Исследователи добавили, что их подход требует дальнейшего совершенствования. Например, их алгоритм основан на обучении с подкреплением без модели, которое требует большого количества данных или большого количества итераций для изучения относительно хорошей политики защиты. В будущем они хотели бы внедрить подходы на основе моделей для ускорения процесса обучения.

Чжу и Лю также работали с Чжишен Ху, бывшим докторантом кафедры электротехники и информатики, а теперь старшим научным сотрудником службы безопасности Baidu Security в Кремниевой долине; Цзюнь Сюй, бывший докторант в области информационных наук и технологий, а ныне доцент Технологического института Стивенса; и Пинг Чен, бывший научный сотрудник, получивший докторскую степень в области информационных наук и технологий, а ныне штатный архитектор безопасности JD.com American Technologies.

Работа была поддержана присуждением премии Междисциплинарной университетской исследовательской инициативы (MURI) Министерства обороны». ***(Machine learning algorithm may be the key to timely, inexpensive cyber-defense // Newswise (https://www.newswise.com/articles/machine-learning-algorithm-may-be-the-key-to-timely-inexpensive-cyber-defense). 04.02.2021).***

***

«AppDynamics (в составе Cisco) представляет Cisco Secure Application — первое решение в отрасли, которое предотвращает кибератаки и обеспечивает сквозную защиту приложений. Новое решение, разработанное совместно с Cisco Security, крупнейшей в мире компанией по обеспечению безопасности на предприятиях, объединяет в единую систему задачи по защите данных и анализу приложений. Решение интегрируется в платформу AppDynamics, позволяя выявлять и автоматически предотвращать угрозы хакерских атак в режиме реального времени, что дает бизнесу уверенность в производительности приложений и уровне клиентского сервиса.

Поскольку в настоящее время организации все чаще взаимодействуют с клиентами дистанционно – через сайты и мобильные приложения – повышается риск утечки персональной информации пользователей и возникновения других инцидентов в области цифровой безопасности. Эта проблема усугубляется ростом числа «удаленных» сотрудников, которые подключают свои устройства к общедоступным сетям. Такая тенденция значительно расширяет ИТ-периметр организаций, создавая новые уязвимости даже в самых защищённых инфраструктурах. Таким образом, отсутствие эффективных решений кибербезопасности не только ставит под угрозу репутацию бренда и доверие клиентов, но также влечет большие финансовые потери для компаний в случае успешной атаки злоумышленников.

В условиях активного использования цифровых технологий, в том числе локальных и мультиоблачных микросервисов, обеспечение информационной

безопасности является первостепенной задачей. Cisco Secure Application позволит техническим специалистам выявлять уязвимости в приложении еще на этапе его разработки, определять их потенциальное влияние на бизнес, а также синхронизировать команды разработки и обеспечения информационной безопасности для быстрого устранения проблемных участков.

С Cisco Secure Application ИТ-команды перестанут рисковать безопасностью конфиденциальной информации ради скорости. Это единственное решение, которое уникальным образом объединяет данные о производительности и безопасности приложений без риска снижения скорости их работы, обеспечивая комплексную защиту от эксплойтов.

«Скорость работы приложения может существенно повлиять на взаимодействие с пользователем, однако безопасность приложения еще более критичный момент — ведь недостаточный уровень защищенности ставит под угрозу личные данные клиента. Компании не могут позволить себе игнорировать этот риск, — отметил Джиту Патель, старший вице-президент и генеральный менеджер бизнес-группы безопасности и приложений Cisco. Cisco Secure Application — это первое решение, обеспечивающее высокую степень безопасности приложений, которое дает компаниям возможность эффективно защищать данные клиентов, гарантируя при этом качественный пользовательский опыт».

Благодаря Secure Application ИТ-команды получают: автоматическую защиту в режиме реального времени: обнаружение хакерских атак, выявление отклонений и своевременную автоматическую блокировку эксплойтов. Упрощенное управление уязвимостями: приложение предоставляет доступ на уровне кода для обнаружения проблемных участков в конфигурации еще на этапе разработки. Анализ безопасности, основанный на бизнес-показателях: параметры безопасности коррелируются с бизнес-процессами, приоритизируя наиболее опасные инциденты. Синхронизация работы команд: возможности синхронизации работы ИТ-сотрудников и специалистов по информационной безопасности с целью повышения эффективности выявления киберугроз и построения здорового цифрового бизнеса.

«ИТ-компании часто думают о том, как преобразовать и синхронизировать между собой системы безопасности и разработки приложений, включая операционные инструменты, процессы и команды, — отметил аналитик IDC, руководитель группы DevOps и I&O Стивен Эллиот. — Сейчас управление уязвимостями приложений является одним из ключевых направлений цифровой трансформации организаций, которое гарантирует значительные преимущества для бизнеса».

Решение Cisco Secure Application в настоящее время доступно в демо-режиме». ***(Владимир Бахур. AppDynamics представила решение для защиты приложений от киберугроз // CNews (https://www.cnews.ru/news/line/2021-02-04_appdynamics_predstavila_reshenie). 04.02.2021).***

***

«Центр интернет-безопасности (CIS), некоммерческая организация, занимающаяся защитой ИТ-систем и данных, объявила о запуске бесплатной

защиты от программ-вымогателей для частных больниц в США с помощью службы блокировки вредоносных доменов и отчетов (MDBR).

Служба MDBR, поддерживаемая системами, поддерживаемыми CIS и Akamai, автоматически блокирует домены, связанные с киберугрозами, включая программы-вымогатели, вредоносное ПО и фишинг, после того, как организации переключают своего поставщика DNS на DNS-сервер Akamai.

«Эта возможность может блокировать подавляющее большинство случаев заражения программами-вымогателями, просто предотвращая первоначальный охват домена доставки программ-вымогателей», - отмечает CIS

CIS будет бесплатно финансировать услуги MDBR для нескольких типов организаций здравоохранения, включая независимые больницы, многобольничные системы, интегрированные системы здравоохранения на базе больниц, учреждения по оказанию пост-неотложной помощи пациентам, психиатрические, реабилитационные и другие специализированные больницы.

Организации общественного здравоохранения, уже защищенные МБРР

MDBR защищает общественные организации здравоохранения, больницы и департаменты здравоохранения при финансировании, предоставленном DHS-CISA через Межгосударственный центр обмена и анализа информации (MS-ISAC).

Эта пилотная программа, финансируемая из федерального бюджета, в настоящее время используется более чем 1000 государственных, местных, племенных и территориальных (SLTT) правительственных организаций США.

«Совет директоров СНГ уделяет приоритетное внимание предоставлению услуг MDBR всем государственным и частным больницам США бесплатно, как через MS-ISAC для государственных больниц, так и через инвестиции в размере 1 млн долларов из средств СНГ для частных больниц в этом году», - Эд Маттисон, исполнительный - сказал вице-президент по операциям и безопасности в странах СНГ.

«CIS полностью финансирует это для частных больниц бесплатно и без каких-либо условий, потому что это правильно, и никто другой не делает это в больших масштабах».

С запуском бесплатной защиты от программ-вымогателей для частных медицинских организаций CIS теперь предоставляет эту услугу бесплатно для всех больниц США.

Уже пресекли некоторые атаки программ-вымогателей

С момента своего запуска MDBR заблокировал миллионы запросов на вредоносные домены, которые могли привести к потенциально успешным атакам или заражениям программ-вымогателей, влияющим на организации SLTT.

Только в декабре 2020 года MDBR заблокировал девять экземпляров доменов-вымогателей для группы из девяти организаций общественного здравоохранения США, предотвратив серьезные киберинциденты, которые могли затронуть сотни тысяч людей.

«Пандемия COVID-19 сделала больницы еще большей мишенью для злонамеренных киберугроз, чем они уже были», - добавил Мэттисон.

«В то время как другие коммерческие организации по кибербезопасности, безусловно, поддерживают больницы и больничные системы, наш некоммерческий

статус и направленность на миссию позволяют нам предлагать эту услугу бесплатно и в любом масштабе для любой больницы или системы, которая может извлечь из этого пользу».

Агентство США по кибербезопасности и безопасности инфраструктуры (CISA), Федеральное бюро расследований (ФБР) и Министерство здравоохранения и социальных служб (HHS) предупредили о неминуемой угрозе киберпреступности больницам и поставщикам медицинских услуг в совместном отчете, опубликованном в конце. октября 2020 г.

Целью рекомендаций было подготовить организации к атакам программ-вымогателей с использованием программ-вымогателей Ryuk и Conti путем обмена тактиками, приемами и процедурами (TTP), характерными для инцидентов, в которых используются эти штаммы вредоносных программ». ***(Sergiu Gatlan. CIS now offers free ransomware protection to all US hospitals // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/cis-now-offers-free-ransomware-protection-to-all-us-hospitals/). 19.02.2021).***

***

«Браузеры на основе Chromium, такие как Microsoft Edge и Google Chrome, скоро будут поддерживать функцию безопасности Intel CET для предотвращения широкого спектра уязвимостей.

Технология Intel Control-flow Enforcement Technology (CET) - это функция безопасности оборудования, впервые представленная в 2016 году и добавленная в процессоры Intel 11-го поколения в 2020 году.

Функция CET предназначена для защиты программ от атак типа Return-Oriented Programming (ROP) и Jump-Oriented Programming (JOP), которые изменяют нормальный поток приложения таким образом, что вместо этого выполняется вредоносный код злоумышленника.

«Атаки JOP или ROP могут быть особенно трудными для обнаружения или предотвращения, потому что злоумышленник использует существующий код, выполняемый из исполняемой памяти, творчески, чтобы изменить поведение программы», - объясняет Байджу Патель из Intel.

Эти уязвимости включают атаки, которые обходят песочницу браузера или выполняют удаленное выполнение кода при посещении веб-сайтов.

Intel CET - это аппаратное решение, которое блокирует эти попытки, вызывая исключения при изменении естественного потока.

Chromium-браузеры, получающие поддержку Intel CET

Windows 10 поддерживает Intel CET с помощью реализации, называемой аппаратной защитой стека.

Чтобы приложения Windows поддерживали эту функцию, они должны быть сначала скомпилированы с флагом компоновщика / CETCOMPAT в Visual Studio. При компиляции с этим флагом программа будет помечена как совместимая с CET Shadow Stack и будет включена защита безопасности.

На этой неделе руководитель исследования уязвимостей Microsoft Edge Джонатан Норман написал в Твиттере, что Microsoft Edge 90 будет поддерживать функцию Intel CET в процессах без отрисовки.

Microsoft Edge, основанный на Chromium, использует несколько процессов для выполнения различных задач.

Согласно твиту Нормана, Intel CET будет использоваться процессами, не связанными с рендерингом, такими как процессы браузера, графического процессора, служебных программ, расширений и подключаемых модулей.

Эта функция безопасности не характерна для Microsoft Edge, но доступна для всех браузеров Chromium, включая Google Chrome, Brave и Opera.

Mozilla также рассматривает возможность добавления поддержки Intel CET в Firefox, но в последнее время не было обновлений статуса их реализации.

Пользователи Windows 10 с процессорами Intel 11-го поколения или процессорами AMD Zen 3 Ryzen, которые также поддерживают CET, могут использовать диспетчер задач Windows, чтобы проверить, использует ли процесс функцию аппаратной безопасности.

Для этого откройте диспетчер задач, перейдите на вкладку «Подробности», щелкните правой кнопкой мыши заголовок столбца и выберите «Выбрать столбцы».

Когда откроется диалоговое окно «Выбрать столбцы», прокрутите вниз и установите флажок «Аппаратная защита стека». После включения в этом столбце будет показано, какие процессы поддерживают функцию безопасности Intel CET…

Ожидается, что Google Chrome и Microsoft Edge 90 будут выпущены 13 апреля 2021 года». ***(Lawrence Abrams. Google Chrome, Microsoft Edge getting this Intel security feature // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/google-chrome-microsoft-edge-getting-this-intel-security-feature/). 14.02.2021).***

***

«Начиная со следующего месяца LastPass больше не позволит использовать бесплатную учетную запись на нескольких типах устройств (компьютерах и мобильных) одновременно.

LastPass - это менеджер паролей, который позволяет синхронизировать и автоматически вводить учетные данные для входа на нескольких платформах, включая Windows, iOS, Android и почти все веб-браузеры.

Хотя LastPass предлагает премиальные подписки с дополнительными функциями, они также предоставляют бесплатную подписку с «управлением паролями с бесплатным доступом на всех ваших устройствах».

Сегодня LastPass начал рассылать клиентам своего бесплатного сервиса по электронной почте новости о том, что с 16 марта 2021 года пользователям больше не будет разрешено использовать сервис одновременно на мобильных и настольных компьютерах.

Вместо этого пользователи будут вынуждены выбрать платформу «Компьютер» или «Мобильное устройство», на которой они хотят использовать бесплатную услугу. Согласно этому письму, пользователи LastPass Free смогут использовать сервис на своих мобильных устройствах Android и iOS одновременно, но не на компьютерах и наоборот.

«Мы вносим изменения в способ доступа пользователей LastPass Free к LastPass на разных типах устройств. LastPass предлагает доступ к двум типам устройств - компьютерам (включая все браузеры, работающие на настольных компьютерах и ноутбуках) или мобильным устройствам (включая мобильные телефоны, умные часы и планшеты).

«Начиная с 16 марта 2021 года LastPass Free будет включать доступ только на неограниченное количество устройств одного типа», - объявил LastPass в бюллетене поддержки.

LastPass Free автоматически выберет указанный тип платформы в зависимости от устройства, на котором вы впервые входите в систему, и после 16 марта. Если вы войдете в систему с телефона, LastPass автоматически установит для вашего активного типа устройства значение «Мобильное».

Хотя пользователи LastPass Free не смогут использовать свои устройства в другой категории устройств, они могут использовать его на неограниченном количестве устройств в той же категории.

Чтобы пользователи не застревали на нежелательной платформе, LastPass предоставляет пользователям три возможности изменить свой активный тип устройства. После третьего изменения пользователи застрянут на этой платформе, если они не обновятся до учетной записи LastPass Premium или Families.

В дополнение к этим новым ограничениям, пользователи Lastpass Free больше не будут получать поддержку по электронной почте и будут иметь доступ только к центру поддержки и форумам LastPass». ***(Lawrence Abrams. LastPass Free to force users to choose between mobile, desktop // (https://www.bleepingcomputer.com/news/security/lastpass-free-to-force-users-to-choose-between-mobile-desktop/). 16.02.2021).***

***

«Microsoft упростит для клиентов Defender для Office 365 идентификацию пользователей и доменов, на которые нацелены фишинговые атаки на основе имитации личности, как недавно было указано в дорожной карте Microsoft 365.

Защитник для Office 365 (ранее известный как Office 365 Advanced Threat Protection) защищает электронную почту корпоративных учетных записей Office 365 от различных угроз, включая, помимо прочего, фишинг учетных данных и компрометацию корпоративной электронной почты.

Олицетворение происходит, когда злоумышленник использует отправителя или домен в сообщении электронной почты, которое очень похоже на реального отправителя или домен (michele@contoso.com вместо michelle@contoso.com и ćóntoso.com вместо contoso.com).

Атаки с имитацией используют эту тактику с конечной целью обмануть получателей, что только что прочитанное электронное письмо пришло из надежного источника.

Новые фильтры обнаружения олицетворения

Администраторы безопасности смогут использовать новые фильтры, получившие название «олицетворенный пользователь» и «олицетворенный домен»,

вместе с обозревателем угроз и обнаружениями в реальном времени для обнаружения пользователей организации и доменов, на которые нацелены атаки имитации.

Эти фильтры добавляют к уже существующим возможностям, которые позволяют получить список фишинговых писем, обнаруженных Защитником для существующих фильтров обнаружения олицетворения Office 365.

«Сегодня мы предоставляем фильтры для технологии обнаружения с олицетворением пользователя или домена, которые отображают все фишинговые электронные письма, обнаруженные с помощью нашего обнаружения олицетворения», - поясняет Microsoft.

«Мы добавляем новые фильтры, называемые олицетворенным пользователем и имитируемым доменом, чтобы позволить группам операций безопасности явно искать конкретных пользователей или домены в своей организации, которые являются целями атак с имитацией имени».

Новая информация будет доступна администраторам группы безопасности на страницах анализа выдачи себя за другое лицо, а также на недавно добавленной странице объекта электронной почты.

Поддержка Microsoft Defender для Office 365 для поиска олицетворенных доменов и пользователей все еще находится в разработке.

Тем не менее, Microsoft работает над тем, чтобы к концу февраля сделать его общедоступным по всему миру во всех средах для всех пользователей Microsoft Defender для Office 365.

Защита от олицетворения не включена по умолчанию

Несмотря на то, что Microsoft Defender для Office 365 поставляется со встроенной защитой от фишинга, защита от олицетворения не настроена и не включена в политике по умолчанию.

Чтобы воспользоваться преимуществами новых возможностей, администраторы также должны включить функции защиты от олицетворения, изменив настройки политик защиты от фишинга по умолчанию.

Позже в этом месяце Microsoft также начнет уведомлять пользователей Microsoft Defender для Office 365 о подозреваемых хакерских атаках на уровне государства, обнаруженных в их клиентах.

Компания также добавила приоритетную защиту учетных записей высокопоставленных сотрудников, в том числе руководителей высшего звена, которые часто становятся объектами атак». ***(Sergiu Gatlan. Office 365 will help admins find impersonation attack targets // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/office-365-will-help-admins-find-impersonation-attack-targets/). 09.02.2021).***

***

«Лаборатория Касперского» выпустила дешифратор для Fonix Ransomware (XONIF), который позволяет жертвам бесплатно восстанавливать свои зашифрованные файлы.

Программа-вымогатель Fonix, также известная как Xinof и FonixCrypter, была запущена в июне 2020 года, но с ноября 2020 года значительно увеличила количество жертв.

В прошлую пятницу один из администраторов программ-вымогателей Fonix написал в Твиттере, что они завершили операцию вымогателя и освободили главный ключ дешифрования.

«Я один из администраторов команды fonix. Вы знаете о команде fonix, но мы пришли к выводу. Мы должны использовать наши возможности в позитивном ключе и помогать другим.

Также полностью удален исходный код rans0mware, но некоторые члены команды не согласны с закрытием проекта, как администратор канала Telegram, который пытается обмануть людей в канале Telegram, продавая поддельный источник и данные. В любом случае теперь главный администратор решил отложить всю предыдущую работу и бесплатно расшифровать все зараженные системы». - FonixTeam

Администратор программы-вымогателя Fonix сообщил BleepingComputer, что за время своей работы они зашифровали от 5000 до 6000 систем.

Вскоре после того, как они поделились расшифровкой, Майкл Гиллеспи подтвердил с помощью BleepingComputer, что ключ действителен и может использоваться для расшифровки файлов жертвы.

Расшифровка FonixRansomware

Хорошая новость заключается в том, что если вы были заражены FonixRansomware, теперь вы можете бесплатно расшифровать свои файлы с помощью обновленной версии RakhniDecryptor от Kaspersky.

Загрузите дешифратор на устройство с зашифрованными файлами и запустите программу. Вам будет предложено согласиться с лицензионным соглашением, и появится основной интерфейс...

Когда вы будете готовы расшифровать файлы, нажмите кнопку «Начать сканирование», и дешифратор попросит вас выбрать зашифрованный файл.

После выбора дешифратор будет искать ваш ключ дешифрования и, когда он будет найден, начнет расшифровывать ваши файлы. BleepingComputer протестировал дешифратор на зашифрованном компьютере и, как вы можете видеть ниже, смог расшифровать файлы.

После того, как вы расшифровали файлы и убедились, что они открываются правильно, вы можете удалить оставшиеся зашифрованные файлы.

Для тех, кому нужна помощь в начале использования дешифратора, сначала прочтите эту страницу, и если это не поможет, не стесняйтесь спросить здесь или связаться с Kaspersky для получения подробной информации о проблеме». ***(Lawrence Abrams. New Fonix ransomware decryptor can recover victim's files for free // Bleeping Computer® (https://www.bleepingcomputer.com/news/security/new-fonix-ransomware-decryptor-can-recover-victims-files-for-free/). 03.02.2021).***

***

«2 февраля компания Canonical представила Ubuntu Core 20, минимальную контейнерную версию Ubuntu 20.04 LTS для устройств и встраиваемых систем Интернета вещей (IoT).

Эта основная версия повышает безопасность устройства за счет безопасной загрузки, полного шифрования диска и безопасного восстановления устройства. Ubuntu Core основывается на экосистеме приложений Ubuntu для создания сверхбезопасных интеллектуальных вещей.

«Каждое подключенное устройство требует гарантированной безопасности платформы и магазина приложений», - сказал Марк Шаттлворт. «Ubuntu Core 20 позволяет новаторам создавать системы с высокой степенью защиты и полностью сосредоточиться на своих уникальных функциях и приложениях, с ограничениями и обновлениями безопасности, встроенными в операционную систему».

Ubuntu Core поддерживает промышленные устройства Интернета вещей. По словам Галема Кайо, менеджера по продукции Canonical, инновационные компании используют его для создания и коммерциализации устройств, ориентированных на потребителей, от кофеварок до медицинских устройств.

Новая версия 20 Ubuntu Core может похвастаться заметными нововведениями в области безопасности устройств. По словам Чарльза Кинга, главного аналитика Pund-IT, с учетом растущего числа и изощренности атак отдельных киберпреступников и киберпреступников, спонсируемых государством, усилия Canonical должны приветствоваться как производителями устройств Интернета вещей, так и их клиентами.

«Фактически, если невозможно обеспечить безопасность удаленных датчиков и подобных устройств, будущее IoT и других встроенных систем под вопросом. Ubuntu Core версии 20 демонстрирует, что Canonical намерена предотвратить такие мрачные сценарии», - сказал он LinuxInsider.

Что делает Core

Ubuntu Core 20 покрывает расходы на проектирование, разработку и обслуживание защищенных устройств, включая регулярные, автоматические и надежные обновления. Canonical работает с поставщиками микросхем и производителями оригинальных разработок (ODM), чтобы оптимизировать весь процесс вывода нового устройства на рынок.

Компания и ее партнеры предлагают «Smart Start» - контракт с фиксированной ценой на запуск устройства, включающего консультации, разработку и обновления для первых 1000 устройств на сертифицированном оборудовании. В результате снижается риск проекта IoT.

Этот выпуск основан на сильных сторонах Ubuntu Core. Обновления безопасности поддерживают контролируемые и автоматические обновления программного обеспечения для автопарков OEM, направленные на то, чтобы исправить «все и везде, быстро».

Кроме того, Ubuntu Core 20 представляет систему восстановления устройств, чтобы минимизировать время простоя из-за обслуживания устройства. Администраторы могут резервировать конфигурацию устройства для восстановления вручную или удаленно, когда это необходимо.

Лучшие функции

Некоторые функции в выпуске версии 20 являются значительными обновлениями более ранней версии. Например, Ubuntu Core 20 улучшает безопасность конечных точек устройства.

Он предоставляет расширенные возможности безопасности, такие как:

Безопасная загрузка: Ubuntu Core 20 загружает только программное обеспечение, которому доверяет производитель устройства, на котором оно работает; и

Полное шифрование диска: Ubuntu Core 20 шифрует данные, хранящиеся на устройствах, для предотвращения несанкционированного доступа.

Безопасность для промышленных пользователей, на которые нацелена Ubuntu Core, отличается от потребительских платформ IoT. Кайо из Canonical отмечает, что последствия нарушений безопасности различны для промышленных и бытовых целей.

«Ubuntu Core обеспечивает такие же расширенные возможности безопасности на уровне ОС для любого устройства, независимо от его использования», - сказал он LinuxInsider.

Уменьшает поверхность атаки

Программное обеспечение обеспечивает минимальную поверхность атаки как для операционной системы, так и для приложений. Это устраняет неиспользуемое программное обеспечение, установленное в базовой ОС, и уменьшает размер и частоту обновлений безопасности.

Все пакеты оснастки, работающие на устройствах Ubuntu Core, строго ограничены и изолированы. Это ограничивает ущерб от взломанного приложения.

Доказуемая целостности программного обеспечения и безопасная загрузка предотвращают несанкционированную установку программного обеспечения с аппаратными корнями доверия. Полное шифрование диска упрощает соблюдение требований конфиденциальности для конфиденциальных потребительских, промышленных, медицинских и интеллектуальных приложений.

«Магазины приложений лежат в основе новой волны бизнес-моделей подключенных устройств», - сказал Кайо. «По мере того, как приложения переходят на периферию, ценность данных в удаленных местах возрастает. В Ubuntu Core 20 добавлена безопасная загрузка с аппаратным шифрованием всего диска, чтобы гарантировать конфиденциальность от физических злоумышленников».

Примеры использования

Bosch Rexroth, поставщик приводов и технологий управления, использует Ubuntu Core для работы своего нового магазина приложений ctrlX Automation. Комбинация ОС Ubuntu Core и снимков создает программно-определяемую промышленную производственную платформу с открытой экосистемой, - предложил Ханс Майкл Краузе, директор по управлению продуктами PLC и IoT в Bosch Rexroth.

«Система обеспечивает более быстрое производство и более надежную безопасность на протяжении всего жизненного цикла устройства. Промышленные машиностроители, использующие эту платформу, могут сломать традиционные

барьеры между информационными технологиями и технологией эксплуатации и освободиться от проприетарных систем», - сказал он.

Intel использует Ubuntu Core, чтобы управлять процессом преобразования розничной торговли, производства, энергетики и здравоохранения с помощью вычислительных платформ нового поколения, специально созданных для интеллектуальных периферийных устройств и Интернета вещей, - добавил Джон Хили, вице-президент Intel в группе Интернета вещей.

«Intel и Canonical сотрудничают, чтобы предоставить Linux премиум-класса. Ubuntu Core поможет OEM-производителям реагировать на постоянно растущий спрос на отраслевые решения IoT, одновременно позволяя ODM быстрее выходить на рынок - и все это за счет долгосрочных поставок и технической поддержки доступность», - сказал он.

Британский благотворительный фонд Raspberry Pi Foundation использует сочетание Raspberry Pi 4 и Ubuntu Core, чтобы передать возможности вычислений и цифрового производства в руки людей во всем мире. По словам Эбена Аптона, основателя Raspberry Pi Foundation и генерального директора Raspberry Pi (Trading) Ltd., Raspberry Pi и Ubuntu способствуют развитию духа обучения, открытий и изобретений в классах и стартапах по всему миру.

«От прототипа с Ubuntu Server на Raspberry Pi 4 до производства с Ubuntu Core на вычислительном модуле Raspberry Pi мы предлагаем следующему поколению изобретателей простой путь ко всему открытому исходному коду», - сказал он.

Что включено

Ubuntu Core является бесплатным и открытым исходным кодом, как и другие настольные и серверные продукты Ubuntu от Canonical. Он коммерциализируется через предложение Smart Start.

Это соглашение с Canonical по фиксированной цене на запуск устройства под управлением Ubuntu Core. Цена включает консультации, разработку и обновления OTA для первых 1000 устройств на сертифицированном оборудовании.

«Предложение Canonical Smart Start нацелено на компании, стремящиеся стать производителями подключенных продуктов, и оно сочетает в себе сертификацию оборудования, программного обеспечения и услуг для ускорения процесса разработки», - сказал Кристиан Рено, директор по исследованиям практики Интернета вещей для 451 Research, часть из S & P Global Market Intelligence.

Он добавил, что компания имеет предварительно сертифицированное оборудование (платы) на базе архитектуры ARM или x86, интегрирована с Raspberry Pi (любой моделью) и предлагает выполнить интеграцию с выбранной клиентом платой, если она не прошла предварительную сертификацию.

Дополнительные параметры Linux для Интернета вещей

По словам Рено, помимо Canonical, Red Hat активно занимается внедрением Linux в IoT / Edge, а также разработчиками проприетарных встроенных ОС.

«Поскольку мы видим, что более надежные вычислительные ресурсы консолидируются на периферии в виде процессоров, оптимизированных для периферии, включая Intel Xeon, или даже Xeon D, или Keem Bay для случаев

использования с низким энергопотреблением, это расширит возможности для Linux на периферии, которые ранее были вне досягаемости микроконтроллеров и ЭБУ с ограниченными вычислительными возможностями в легковых автомобилях», - сказал он LinuxInsider.

Десятки тысяч промышленных и потребительских устройств IoT работают под управлением Ubuntu Core, выпущенного на рынок компаниями Bosch Rexroth, Dell, ABB, Rigado, Plus One Robotics, Jabil и другими, отмечает Canonical». ***(Jack M. Germain. Ubuntu Core 20 Brings Better Industrial IoT Control // ECT News Network (https://www.technewsworld.com/story/87004.html). 02.02.2021).***

***

«Компания WhiteHat Security, провайдер безопасности приложений, выпустила AppSec Stats Flash Volume 2. AppSec Stats Flash от WhiteHat дебютировал в прошлом месяце и представляет собой новый ежемесячный современный подкаст и формат отчетов, который обеспечивает более точное представление о текущем состоянии безопасности приложений. В эпизоде этого месяца к Сету Кулкарни из WhiteHat Security, вице-президенту по корпоративной стратегии и развитию бизнеса, и Заку Джонсу, старшему директору по исследованиям в области обнаружения, присоединился Алан Снайдер, генеральный директор NowSecure, чтобы обсудить состояние безопасности мобильных приложений, изучив данные обнаружения и вероятность уязвимости.

«В 2021 году у нас будет больше подробных данных о безопасности и взломах, чем когда-либо прежде. Тем не менее, состояние безопасности приложений остается очень тревожным. Ни одно приложение не создается одинаково, и поэтому каждое представляет собой совершенно уникальную поверхность для атаки», - сказал Кулкарни. «Это, в сочетании с тем фактом, что сегодня приложения становятся все более полиморфными, представляя веб-интерфейсы, мобильные интерфейсы и интерфейсы на основе API, делает безопасность приложений сложной задачей».

Дополнительные результаты включают:

Исследования показали, что не менее 50% приложений в таких отраслях, как производство, общественные услуги, здравоохранение, розничная торговля, образование и коммунальные услуги, уязвимы в течение года из-за одной или нескольких серьезных уязвимостей, которыми можно воспользоваться.

Анализ данных показал, что по мере того, как все больше отраслей стремятся стать онлайн-первыми, окно уязвимости продолжает оставаться ненормально высоким, что приводит к увеличению уязвимости.

С прошлого месяца статистика показала, что 12-месячное скользящее среднее время исправления критических приложений сократилось до 189 дней с 194 дней.

В февральском выпуске журнала WhiteHat Security AppSec Stats Flash было обнаружено, что только пять из десяти наиболее распространенных обнаружений рисков WhiteHat представлены в OWASP Top 10.

Джонс добавил: «Существует интересное различие между образовательным инструментом из списка OWASP Top 10 и уязвимостями, которые мы видим в WhiteHat, которые чаще всего обнаруживаются в приложениях». ***(Research reveals***

50% of apps have security vulnerabilities // BNP Media (https://www.securitymagazine.com/articles/94639-research-reveals-50-of-apps-have-security-vulnerabilities). 19.02.2021).

***

Питання криптографії

«Специалисты швейцарской IT-компании Terra Quantum AG с помощью квантового компьютера выявили уязвимости в криптографическом алгоритме AES. Используя метод, известный как квантовый отжиг, компания доказала, что даже самые сильные версии AES могут быть расшифрованы квантовыми компьютерами в течение нескольких лет.

Предположительно, данные проблемы ставят под угрозу конфиденциальность данных в Сети, банковских транзакций и электронной почты, а также потенциально могут привести к опасным последствиям для таких техногигантов, как Google, Microsoft и IBM.

По словам экспертов, проблемы были обнаружены в симметричном алгоритме блочного шифрования Advanced Encryption Standard (AES). Как отметил директор Terra Quantum AG Маркус Пфлич (Markus Pflitsch), им удалось с помощью квантового компьютера не только зафиксировать, но также доказать небезопасность алгоритма шифрования.

AES был принят в качестве стандарта шифрования правительством США. В июне 2003 года Агентство национальной безопасности США постановило, что шифр AES является достаточно надежным, чтобы использовать его для защиты сведений, составляющих государственную тайну». ***(Квантовый компьютер выявил уязвимости в AES шифровании // SecurityLab.ru (https://www.securitylab.ru/news/516323.php). 08.02.2021).***

***